

recommends FINRA members maintain awareness of this threat and remain vigilant for fraudulent websites, suspicious phone calls, and phishing emails that could be associated with this emerging campaign. Additionally, before entering any login credentials or sensitive information into a website, verify the URL to ensure it is legitimate. More information about this threat, including reporting and mitigation guidance, is available in FINRA's [Regulatory Notice 20-30](#).

Federal Partner Announcements



CISA Releases 5G Strategy

The Cybersecurity and Infrastructure Security Agency (CISA) has released the [CISA 5G Strategy](#), which details the Agency's plan to advance the development and deployment of a secure and resilient fifth generation (5G) infrastructure.

The Strategy establishes five strategic initiatives that stem from the four Lines of Effort defined in the [National Strategy to Secure 5G](#) and seeks to promote the development and deployment of 5G infrastructure, one that enables enhanced national security, technological innovation, and economic opportunity for the United States and its allied partners. Guided by three core competencies of risk management, stakeholder engagement, and technical assistance—these initiatives include associated objectives to ensure there are policy, legal, security, and safety frameworks in place to fully leverage 5G technology while managing its significant risks.

In addition to the Strategy, CISA has released a [5G Basics Infographic](#) to educate stakeholders on key challenges and risks associated with the emerging technology. Working in close collaboration with our stakeholder community, the Agency plans to publish [sector-specific](#) 5G risk profiles in the coming months. We look forward to engaging with you on the sector profiles to gather your feedback.

To learn more about CISA's role in 5G and to view the strategy, visit www.cisa.gov/5G.

Current and Emerging Cyber Threats

New QakBot Campaign Uses Endpoint Detection Evasion Techniques

Security researchers discovered an update in the QakBot/QBot banking Trojan within its most recent phishing campaign that leverages a persistence mechanism to remain undetected by antivirus software and avoid manual analysis. This campaign sends phishing emails containing a ZIP file to bypass malware detection features in email security gateways. Within this ZIP file is a Word document embedded with malicious macros. If a victim enables these macros by clicking “Enable Editing” on the document, the malware contained within it will execute a PowerShell script and download the latest QakBot payload. This sophisticated attack contains several features that allow it to bypass endpoint detection tools, including the use of AutoOpen and AutoClose triggered functions and explorer[.].exe. To prevent further analysis, the batch script included in the malicious document kills processes and deletes artifacts from the infected machine. *The NTIC Cyber Center recommends users remain vigilant for this and other QakBot email campaigns, avoid opening and unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. If you believe you have been infected with QakBot, notify your organization’s IT security team immediately so they may contain and remediate the infection. We recommend network administrators proactively block the associated IoCs provided in [Morphisec’s report](#).*

Hacking Campaign Actively Targeting Discount Rules for WooCommerce WordPress Plugin

A hacking campaign is currently [targeting](#) websites using an unpatched version of the Discount Rules for WooCommerce WordPress plugin. These attacks are attempting to exploit SQL injection and unauthenticated stored cross-site scripting (XSS) security vulnerabilities that exist within older versions of the plugin to compromise websites and steal data. Researchers noted that most of the attacks targeting the vulnerable plugin originate from IP address 45[.]140[.]167[.]17. While a patch that addresses these vulnerabilities has been released, there are still at least 17,000 websites running the unpatched version of the plugin, making them vulnerable to exploitation. *The NTIC Cyber Center recommends WordPress website administrators using the Discount Rules for WooCommerce plugin update it to version 2.1.0 immediately. Changing the affected website’s administrator password, enabling two-factor authentication, and properly vetting all plugins prior to and after installation is also recommended.*

Malware Discovered in Amazon Machine Images

Researchers at cybersecurity company Mitiga [discovered](#) Amazon Machine Images (AMIs) laced with malicious code on the Amazon Web Services (AWS) Marketplace that could lead to a compromised cloud environment. In one incident, an Elastic Compute Cloud (EC2) instance within an organization's AWS environment was embedded with an active cryptocurrency miner. This

resulted in an increase in the victim's cloud hosting bill due to the excessive processing power used by the malware. *The NTIC Cyber Center recommends that administrators only use AMIs from trusted and vetted sources and test all AMIs in a sandboxed environment before launching them in a business-critical environment.*

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data at risk. Our goal is to keep you informed of the latest ransomware threats and provide important information to help you thwart these types of attacks. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

DarkSide Ransomware Campaign Targets Organizations with Customized Executables, Threatens to Publish Stolen Data

A new human-operated ransomware campaign, dubbed DarkSide, [emerged](#) around August 10, 2020, targeting organizations with customized ransomware executables. Once the ransomware is executed on a system, it launches a PowerShell command that deletes Shadow Volume Copies to prevent the victim from restoring files. It then terminates various databases, office applications, and email clients, while avoiding certain processes and applications that could be used to connect to infected systems. The DarkSide threat actors will also move laterally throughout the network, harvesting unencrypted data and gaining access to an administrator account and the Windows domain controller. The stolen data is then used to coerce victims into paying the ransom under the threat of it being publicly released. According to recent victims, DarkSide ransomware operators demand anywhere from \$200,000 to \$2,000,000 to decrypt files and delete stolen data. While not validated, DarkSide operators claim that they do not target organizations within the following sectors: healthcare, education, non-profit organizations, and government agencies. There is currently no free decryption tool available for this variant.

Low-Skilled Iranian Hacking Group Deploying Dharma Ransomware against Organizations

Security firm Group-IB has [identified](#) a new group of low-skilled hackers reportedly operating out of Iran that have been using Dharma ransomware to launch attacks against companies in Russia, Japan, China, and India. This unnamed group appears to use publicly available hacking tools

available on GitHub or downloaded from Telegram hacking channels, including Masscan, NLBrute, Advanced Port Scanner, Defender Control, and Your Uninstaller. Group-IB notes that the group prefers to brute-force Remote Desktop Protocol (RDP) endpoints to gain access to a target's network likely because it is easy to identify and exploit RDP systems. This group requests smaller ransom amounts ranging between one and five Bitcoin (\$10,000 to \$50,000), rather than larger amounts that would gain the attention of law enforcement and reduce the likelihood of being paid.

Data Leaks and Breaches

Freepik and Flaticon

Photo and graphics site Freepik along with sister site Flaticon [disclosed](#) a breach in which millions of user accounts were affected. Information compromised in the breach includes email addresses and hashed passwords. The breach is attributed to threat actors leveraging an SQL injection vulnerability to gain access to the target database. The parent company has since distributed data breach notifications urging affected users to change their credentials. ***The NTIC Cyber Center recommends that affected Freepik and Flaticon users change their credentials, monitor their accounts for any unauthorized or suspicious activity, and enable multifactor authentication on any account that offers it.***

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



Disaster scams are a type of social engineering scheme in which perpetrators target and defraud victims of natural disasters, severe weather events, or other catastrophic occurrences. These scams attempt to further victimize those struggling to recover from incidents such as floods, hurricanes, wildfires, and tornadoes, although scammers are known to exploit victims in the wake of nearly any emergency situation. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

[Cybersecurity Experts Issue Warnings as Schools Begin Remotely, Businesses Continue Work Online Amid COVID-19](#)

Analytic Comment: With many schools beginning fall classes online and businesses remaining in a telework posture for the foreseeable future, cybersecurity must become and remain a priority for organizations, as end users are increasingly vulnerable to attacks. Throughout the pandemic, cyber threat actors have shifted their focus to targeting end users who are no longer protected by their organization's network security controls. This has resulted in an increase in social engineering attacks such as phishing and vishing designed to steal online account credentials and other sensitive data. To help employees recognize and avoid these threats while away from the office, regular cybersecurity and cyber threat awareness training is highly encouraged.

Patches and Updates

[Google Releases Security Updates for Chrome](#)

ICS-CERT Advisories

[Advantech iView](#)

[Emerson OpenEnterprise](#)

[Philips SureSigns VS4](#)

[Treck TCP/IP Stack \(Update G\)](#)

[WECON LeviStudioU](#)

We welcome your feedback.

Please click [here](#) to complete a brief survey and let us know how we're doing.

Receive this email from a friend or colleague and want to subscribe? Sign up [here](#)!

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.





NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Weekly Cyber Threat Bulletin

TLP:WHITE

Product No. 2020-09-004

HSEC-1 | NTIC SIN No. 2.5, 5.4

September 3, 2020

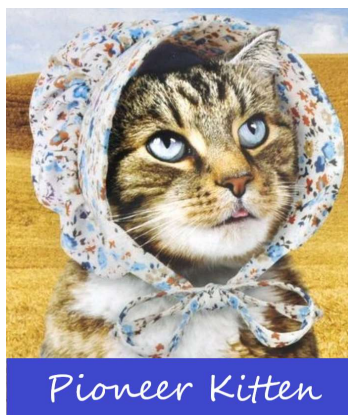
National Capital Region Cyber Threat Spotlight



Iranian APT Group Charming Kitten Uses LinkedIn and WhatsApp to Target Victims

According to a recent [report](#) from cybersecurity firm Clearsky, members of the Iranian cyber-espionage group "Charming Kitten," also known as APT35, have been posing as journalists on LinkedIn and on the WhatsApp call and messaging platform to establish contact with targets such as human rights activists, people in academia, and journalists who specialize in Iranian issues and affairs. After contact is made with a target via LinkedIn, the hacker then tries to schedule a call via WhatsApp to gain that person's trust. After the call, the hacker sends the target a link to a compromised "Deutsche Welle" domain that hosts either a phishing page or a ZIP file containing malware designed to steal the target's credentials. Researchers have classified this recent operation as an upgrade from attacks Charming Kitten deployed in 2019, when this same threat group posed as reporters from the Wall Street Journal. *The NTIC Cyber Center recommends users remain vigilant for phishing attempts disguised as requests from media representatives and journalists,*

avoid opening unexpected emails and social media messages, and refrain from clicking on links and opening attachments from unknown or untrusted sources. We also recommend scrutinizing any unsolicited request to communicate solely via WhatsApp, as the platform has become an attractive tool for criminals and scammers due to its encryption and privacy features.



Iranian APT Group Pioneer Kitten Selling Access to Compromised Corporate Networks

The Iranian advanced persistent threat (APT) group known as Pioneer Kitten ([CrowdStrike](#)), Fox Kitten ([ClearSky](#)), and Parisite ([Dragos](#)) was observed on underground forums selling access to compromised corporate networks and targeting F5 BIG-IP devices vulnerable to [CVE-2020-5902](#) exploits. CrowdStrike claims that Pioneer Kitten is likely contracted by the Iranian government and is largely fixated on gaining unauthorized access to sensitive information that may be of interest to Iranian government officials. Pioneer Kitten was observed in July 2020 attempting to sell access to compromised networks to other threat actors and has previously provided unauthorized network access to other Iranian-sponsored cyber threat actors. Although F5 has released a patch for CVE-2020-5902, Pioneer Kitten adjusted their operations to identify and target organizations that have not yet applied the patch. *The NTIC Cyber Center encourages all organizations encrypt critical and sensitive data both in transit and at rest, regularly audit third-party access to networks, and audit networks for unauthorized access and exposed ports. We also recommend all network administrators review the Cybersecurity and Infrastructure Security Agency's Alert [AA20-206A](#), review the associated mitigation strategies, and apply the corresponding patches as soon as possible.*

Federal Partner Announcements



FBI Warns of Fraud Trend: Online Romance Scams

The Federal Bureau of Investigation is working to raise [awareness](#) about online romance scams, also called confidence fraud, specifically among single adults over the age of 55 in Utah, Idaho, and Montana. In this type of fraud, scammers take advantage of people looking for romantic partners on dating websites, apps, or social media, with the ultimate goal of financially exploiting the victims.

The consequences of these scams are often financially and emotionally devastating to victims; they rarely get their money back and may not have the ability to recover from the financial loss.

According to the FBI's Internet Crime Complaint Center (IC3), which provides the public with a means of reporting Internet-facilitated crimes, romance scams result in greater financial losses to victims when compared to other online crimes. In 2019, almost 20,000 complaints categorized as romance scams were reported to IC3 (about 1,000 more than the previous year), and the losses associated with those complaints exceeded \$475 million. In Idaho last year, the IC3 received nearly 100 complaints from victims reporting more than \$1 million in losses related to romance scams.

The criminals who carry out romance scams are experts at what they do. If you develop a romantic relationship with someone you meet online, consider the following:

- Research the person's photo and profile using online searches to see if the material has been used elsewhere.
- Go slow and ask questions.
- Beware if the individual seems too perfect or quickly asks you to leave a dating service or social media site to go "offline."
- Beware if the individual attempts to isolate you from friends and family or requests.
- Beware if the individual promises to meet in person, but then always comes up with an excuse why he or she can't. If you haven't met the person after a few months, for whatever reason, you have good reason to be suspicious.
- Never send money to anyone you don't know personally.

If you believe you are a victim of a romance scam, stop all contact immediately and file a complaint online at www.ic3.gov. For more information about this threat, please see the NTIC Cyber Center's product titled [Securing Our Communities: Romance Scams](#).



September Is National Insider Threat Awareness Month

September is National Insider Threat Awareness Month (NIATM), which is a collaborative effort between the National Counterintelligence and Security Center (NCSC), National Insider Threat Task Force (NITTF), Office of the Under Secretary of Defense Intelligence and Security (USD(I&S)), Department of Homeland Security (DHS), and Defense Counterintelligence and Security Agency (DCSA) to emphasize the importance of detecting, deterring, and reporting insider threats.

NITAM 2020 will focus on “Resilience” by promoting personal and organizational resilience to mitigate risks posed by insider threats. The Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to read [NCSC’s NITAM 2020 endorsement](#) and explore the following resources to learn how to protect against insider threats:

- [Insider Threat Mitigation](#)
 - [CISA Webinar: A Holistic Approach to Mitigating Insider Threats](#)
 - [NITTF Resource Library](#)
 - [Center for Development of Security Excellence: Insider Threat Awareness and Training](#)
-

Current and Emerging Cyber Threats

UltraRank Threat Group Uses JS Sniffers to Steal Payment Card Information Entered on Hundreds of Ecommerce Websites

Researchers at Group-IB have [uncovered](#) a threat actor dubbed UltraRank that uses JavaScript sniffer malware to compromise ecommerce sites or online suppliers to steal their customer payment card data. JavaScript Sniffers pilfer financial data at the point of purchase on these ecommerce sites and UltraRank has compromised approximately 700 websites and 13 service providers from various countries. UltraRank has often changed its infrastructure and malicious code to steal payment card data and they have been observed to be leveraging the FakeLogistics, WebRank and SnifLite malware families. *The NTIC Cyber Center recommends website visitors remain vigilant for indications that a webpage may be compromised. These may include being asked twice to enter payment or login information or being prompted for payment card details before being forwarded to a secure payment service provider. Customers making purchases on ecommerce platforms*

should routinely monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity. In addition, we recommend ecommerce website administrators regularly test web applications for vulnerabilities, implement file integrity monitoring or change-detection software, perform periodic penetration testing to identify weaknesses, and keep anti-malware solutions and security patches up to date. As these attacks are similar to ones conducted by Magecart groups, we recommend reviewing our product titled [Magecart: A Rapidly Growing Threat to Ecommerce Websites](#).

Hacking Campaign Targets Unpatched QNAP NAS Devices

Researchers recently [discovered](#) a hacking campaign that exploits a three-year-old remote command execution (RCE) vulnerability present in unpatched firmware of QNAP network attached storage (NAS) devices. This RCE vulnerability allows unauthenticated threat actors to remotely gain access to the device and deploy malware such as ransomware. The vulnerability is attributed to a command injection weakness allowing threat actors to leverage the authLogout.cgi executable due to a failure to sanitize inputs. The motive of this campaign is currently unknown. *The NTIC Cyber Center recommends administrators of QNAP NAS devices are encouraged to review this [security advisory](#) and apply the appropriate firmware updates to patch against these vulnerabilities as soon as possible.*



Emotet's New Red Dawn Email Attachment

Synopsis: After a five-month hiatus, the [Emotet](#) botnet is generating a massive surge in malicious phishing emails worldwide using a new malicious attachment template, dubbed "Red Dawn."

Masquerades as: Invoices, shipping information, COVID-19 information, resumes, financial documents, scanned documents

Sectors Targeted: All

Motive: Delivers additional malware such as Trickbot, QBot, and ransomware

Threat Actor(s)/Origin: [TA542](#)

Platforms Affected: Windows

QBot Steals Reply-Chain Emails

Synopsis: Threat actors are hijacking reply-chain emails to distribute the [QBot/QakBot](#) banking and information-stealing Trojan. QBot can steal passwords, cookies, credit cards, emails, online banking credentials and deploy additional malware.

Masquerades as: Legitimate emails within an email reply-chain

Sectors Targeted: All

Motive: Profit-motivated, delivers additional malware, conducts data theft

Threat Actor(s)/Origin: Unknown

Platforms Affected: Windows

Instagram Phishing Scam

Synopsis: A new Instagram [phishing scam](#) uses malicious direct messages to target high-profile Instagram users and steal their email addresses, login credentials, and dates of birth.

Masquerades as: Instagram Help Center

Sectors/Persons Targeted: Entertainment & Media/High-Profile Social Media Users

Motive: Data theft

Threat Actor(s)/Origin: Unidentified Turkish-speaking cybercriminals

Platforms Affected: Instagram

Mitigation recommendations: The NTIC Cyber Center recommends users remain vigilant for these and other phishing campaigns and be wary of unexpected emails, text messages, and social media messages. Additionally, refrain from clicking on links or opening attachments sent from unknown or untrusted sources and never enable content or macros on Microsoft Office documents before verifying their legitimacy. If you believe you have been infected with malware or have had your login credentials stolen as a result of a phishing campaign, notify your organization's IT security team immediately. To learn how to identify phishing emails, please see the NTIC Cyber Center's product titled [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

New and Notable Malware Campaigns

Lucifer Cryptomining DDoS Malware

Synopsis: [Lucifer](#), a cryptomining and distributed denial-of-service (DDoS) botnet malware that previously only infected Windows systems, can now target and infect Linux systems.

Sectors Targeted: All

Motive: Profit-Motivated

Threat Actor(s)/Origin: Unknown

Platforms Affected: [Windows](#), [Linux](#)

Attack Vector(s): Vulnerability exploitation, brute-forcing systems via TCP port 135 (RCP) and 1433 (MSSQL)

Associated CVEs: [CVE-2014-6287](#), [CVE-2018-1000861](#), [CVE-2017-10271](#), [ThinkPHP RCE vulnerability \(CVE-2018-20062\)](#), [CVE-2018-7600](#), [CVE-2017-9791](#), [CVE-2019-9081](#), [PHPStudy Backdoor RCE](#), [CVE-2017-0144](#), [CVE-2017-0145](#), [CVE-2017-8464](#)

Mitigation Recommendations: Ensure servers and operating systems are up to date with the latest patches; close any unneeded ports; replace default usernames with something unique, make sure passwords are lengthy, complex, and unique to each account, and enable multifactor authentication; proactively block IoCs contained in this report: [NetScout – Lucifer’s Spawn](#).

Lemon_Duck Cryptomining Malware

Synopsis: [Lemon_Duck](#), a cryptomining malware that previously only infected Windows, now also targets and infects Redis instances and Hadoop clusters.

Sectors Targeted: All

Motive: Profit-Motivated

Threat Actor(s)/Origin: Unknown

Platforms Affected: [Windows](#), [Linux](#) servers running Redis and Hadoop

Attack Vector(s): COVID-19-themed phishing emails, vulnerability exploitation, SSH brute-force, binary brute-force using EternalBlue exploit

Associated CVEs: [CVE-2017-8570](#), [CVE-2020-0796](#), [CVE-2017-8464](#)

Mitigation Recommendations: Ensure servers and operating systems are up to date with the latest patches; close any unneeded ports; properly configure and [secure SSH servers](#), replace default usernames with something unique, make sure passwords are lengthy, complex, and unique to each account, and enable multifactor authentication; proactively block IoCs contained in this report: [SophosNews – Lemon_Duck Cryptominer Targets Cloud Apps & Linux](#).

Cetus Cryptomining Malware

Synopsis: [Cetus](#) is a new cryptomining malware that mines Monero cryptocurrency and masquerades as legitimate Docker binaries to remain hidden.

Sectors Targeted: Unknown

Motive: Profit-Motivated

Threat Actor(s)/Origin: Unknown

Platforms Affected: Docker

Attack Vector: Exploitation of unsecured Docker daemon instances

Associated CVEs: N/A

Mitigation Recommendations: Review [Docker's security guidance](#) and properly secure [Docker daemon sockets](#), secure all cloud administrator accounts with lengthy, complex and unique passwords, and enable multifactor authentication; proactively block IoCs contained in this report: [Cetus: Cryptojacking Worm Targeting Docker Daemons](#).

Vulnerabilities

Cisco IOS XR Software

Cisco issued a [warning](#) about a new zero-day vulnerability ([CVE-2020-3566](#)) impacting the Distance Vector Multicast Routing Protocol (DVMRP) feature in their Internetwork Operating System (IOS) XR equipment. This vulnerability, if exploited, can provide threat actors unauthenticated remote access and allow them to cause the process memory to crash, closing all processes running on the compromised device. This vulnerability can compromise any Cisco device running IOS XR Software with multicast routing enabled on its interface. There are currently no patches available. *The NTIC Cyber Center recommends administrators of affected devices review [Cisco's Security Advisory](#) for indicators of compromise (IoCs) and mitigation strategies.*

File Manager WordPress Plugin

Unknown hackers are actively targeting and exploiting a critical remote code execution vulnerability present in the File Manager WordPress plugin versions 6.0 through 6.8. According to the WordPress website, more than 700,000 websites have the File Manager plugin installed and the WordPress security firm, Wordfence [reports](#) blocking over 450,000 exploit attempts in the past few days. If exploited, this vulnerability can allow attackers to manipulate website files and potentially escalate privileges in the website's admin area. The developers of the File Manager plugin released an update to patch this vulnerability. *The NTIC Cyber Center recommends all WordPress website administrators using the File Manager plugin update to version 6.9 immediately.*

Data Leaks and Breaches



The American Payroll Association (APA), a nonprofit professional association, [disclosed](#) a breach affecting member and customer data. Information compromised in the breach includes usernames, passwords, payment card data, social media usernames and profile photos. The breach is attributed to a web skimmer planted on the organization's website login and online store checkout pages. The APA has since reset passwords for affected users and is offering free Equifax credit monitoring. ***The NTIC Cyber Center encourages those affected to consider placing a fraud alert or security freeze on their credit files and activating the free credit monitoring services offered to affected customers and members. Additionally, website visitors remain vigilant for indications that a webpage may be compromised. These may include being asked twice to enter payment or login information or being prompted for payment card details before being forwarded to a secure payment service provider.***

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



Business Email Compromise (BEC) – also known as a **CEO scam** or **whaling** – is a type of phishing scheme in which the perpetrator conducts online reconnaissance against a target organization and then uses various social engineering techniques to try and convince employees within that organization to divulge sensitive personal or financial information. This scheme is successful when the perpetrators can elicit an emotional response from their targets that overrides

logic and any security procedures the organization already has in place. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

[Elon Musk Confirms Russian Hacking Plot Targeted Tesla Factory](#)

Analytic Comment: A Russian national was arrested for traveling to the US and attempting to recruit a Tesla employee for one million dollars in exchange for infecting Tesla's systems with malware. The employee notified Tesla and the FBI of this attempt. The foreign national was part of a Russian-based hacking group that wanted use malware to steal information from Tesla and demand a ransom. This incident underscores the importance of employing trustworthy individuals and implementing organizational policies and audits to reduce the risk that insider threats can pose.

[State Voter Registration Systems Have Not Been Hacked, Officials Say](#)

Analytic Comment: To quell fears of compromise, federal and state officials announced that no state voter registration databases have been hacked this year. Doubts of this arose as a viral Russian news article claimed a hacker acquired personal voter data belonging to 7.6 million individuals from Michigan. However, most voter registration data is public information and can be legally obtained. While it is plausible that a foreign election influence campaign would leverage legally accessible voter registration data, voters are encouraged to think critically and consume news and media from trusted and vetted sources.

[Local Government Organizations Most Frequently Targeted by Ransomware](#)

Analytic Comment: According to a Barracuda Networks report, 44 percent of ransomware attacks that have taken place this year have targeted local governments, making it the most frequently targeted sector by ransomware threat actors. Subsequently, 15 percent of local government organizations affected by ransomware have confirmed that they have made payments to threat actors. Researchers have also noticed a surge in ransomware attacks against the education and healthcare sectors, due to cyber-criminals taking advantage of the COVID-19 pandemic. This underscores the importance of local governments developing the ability to effectively use machine learning-enabled software to mitigate technical and human errors. Local government network administrators should continue subscribing to IP blacklists, use advanced firewalls and malware detection tools while positively enforcing cyber awareness trainings for employees. Implementing a robust data backup policy is also highly recommended.

Patches and Updates

[Cisco Releases Security Updates](#)

ICS-CERT Advisories

[Mitsubishi Electric Multiple Products](#)

[OpenClinic GA \(Update A\)](#)

[Red Lion N-Tron 702-W, 702M12-W](#)

We welcome your feedback.

Please click [here](#) to complete a brief survey and let us know how we're doing.

Receive this email from a friend or colleague and want to subscribe? Sign up [here](#)!

TLP:WHITE

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up at one of our events, or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.





NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM

Cyber Center

Weekly Cyber Threat Bulletin

10 September 2020
Product No. 2020-09-014
NTIC SIN No. 2.5 | HSEC SIN No. 1

National Capital Region Cyber Threat Spotlight

[REDACTED], we found a package from March pending for you. Kindly assume ownership and confirm for delivery here: l5ssv.info/QTGGdgoLks

Takoma Park Police Department Warns of Smishing Scam

On September 3, 2020, the Takoma Park Police Department in Maryland issued a [warning](#) via their Twitter account about a “Package Pending” smishing scam targeting residents. Smishing is a type of phishing campaign that uses text messages, or SMS messages, to target mobile phone users. These messages often contain links to malicious websites or apps that can infect mobile phones with malware or steal victims’ personal information. *The NTIC Cyber Center recommends all mobile phone users maintain awareness of this and other smishing campaigns and avoid clicking on links in unexpected or unsolicited text messages. For more information on how to identify smishing and other phishing threats, please see our product titled [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).*

Federal Partner Announcements



CISA
CYBER+INFRASTRUCTURE

DHS Combats Potential Electromagnetic Pulse (EMP) Attack

In accordance with Executive Order 13865, the Department of Homeland Security (DHS)—through CISA and in coordination with the interagency—is taking key actions to address known EMP-related vulnerabilities to critical infrastructure.

The EMP Program Status Report addresses efforts taken by DHS to foster increased resilience to EMP events through vulnerability assessments, testing and pilot programs, data analysis and validation, risk assessments, and public and private sector coordination. For more information, please see CISA's EMP Program Status Report [here](#).

TLP: WHITE

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Current and Emerging Cyber Threats

Hacker Selling Compromised RDP Accounts of Healthcare Sector Organizations

According to a Nuspire [report](#), a hacker known as “TrueFighter” has been targeting the remote desktop protocol (RDP) of industries across all sectors with healthcare as the key target. “TrueFighter” reportedly works alone and is known for breaching networks and then selling the stolen credentials on the dark web for financial gain. Additionally, “TrueFighter” sells information on the dark web outlining how to obtain remote administrative access on the already compromised RDP accounts, defining the industry that was infiltrated. ***The NTIC Cyber Center recommends all network administrators proactively block connections to unneeded RDP ports, secure necessary RDP ports by implementing IP address whitelisting, and securing associated accounts with unique, secure passwords and multifactor authentication. We also recommend requiring the use of a Virtual Private Network (VPN) to connect to any internal resources and monitoring networks for suspicious activity and unauthorized access.***

TeamTNT Abuses Legitimate Cloud Monitoring Tools to Breach Cloud Infrastructure

Cybersecurity firm Intezer recently discovered a cybercrime group, dubbed TeamTNT, abusing legitimate cloud monitoring tools such as Weave Scope to target and gain unauthorized access to cloud computing environments. Weave Scope is an open source tool that is integrated with Docker, Kubernetes, the Distributed Cloud Operating System, and AWS Elastic Computer Cloud. When abused, attackers can use this tool to map and gain full control over everything within their target’s cloud environment, creating a backdoor that can allow the execution of system commands without needing to infect the cloud server with malware. ***The NTIC Cyber Center recommends all administrators of cloud environments close or restrict access to exposed Docker API ports, block incoming connections to port 4040, and proactively block the associated indicators of compromise (IoCs) available in Intezer’s [report](#).***

New Baka JavaScript Skimmer Discovered on Merchant Websites

Researchers working on Visa's Payment Fraud Disruption initiative [warn](#) of a new JavaScript ecommerce skimmer, dubbed Baka, that targets site visitors’ payment card data entered into checkout pages of online stores. Once Baka is added to a checkout page, its loader downloads the skimming code from the attacker’s command-and-control (C2) server and executes it within the customer’s system memory. After the skimmer steals the customer’s payment card data, Baka removes itself from memory. These methods are used to evade detection by both the merchant and the customer. ***The NTIC Cyber Center recommends website visitors remain vigilant for indications that a webpage may be compromised. These may include being asked twice to enter payment or login information or being prompted for payment card details before being forwarded to a secure payment service provider. Customers making purchases on ecommerce platforms should routinely monitor their account statements and immediately notify their financial institutions of any unauthorized or suspicious activity. In addition, we recommend ecommerce website administrators regularly test web applications for vulnerabilities, implement file integrity monitoring or change-detection software, perform periodic penetration testing to identify weaknesses, and keep anti-malware solutions and security patches up to date. As these attacks are similar to ones conducted by Magecart groups, we recommend reviewing our product titled [Magecart: A Rapidly Growing Threat to Ecommerce Websites](#).***



TA2719 Phishing Campaign Delivers NanoCore and AsyncRAT

Synopsis: Proofpoint researchers are investigating a new phishing campaign in which threat actors use emails embedded with colorful images, malicious attachments, and poisoned links to deliver Remote Access Trojans (RATs) NanoCore and AsyncRAT to victims. The known locations affected by this campaign include the United States, Austria, Chile, Greece, Hungary, Italy, North Macedonia, Netherlands, Spain, Sweden, Taiwan, and Uruguay.

Masquerades as: Banks, law enforcement, purchase orders, and shipping services

Sectors Targeted: All

Motive: To gain remote access to victims' systems and networks

Threat Actor(s)/Origin: TA2719

Platforms Affected: Windows

Report: [Proofpoint](#)

New Emotet Phishing Campaign Masquerades as Windows 10 Mobile OS Notification

Synopsis: A new phishing campaign uses the Windows 10 Mobile operating system (OS) as a lure to deliver Emotet via Word document attachments containing malicious macros.

Masquerades as: A Windows 10 Mobile OS notification

Sectors Targeted: All

Motive: To infect systems with Emotet and deliver additional malware such as Trickbot, QBot, and ransomware

Threat Actor(s)/Origin: Unknown

Platforms Affected: Windows

Report: [BleepingComputer](#)

Phishing Campaign Masquerades as Technical Support Team to Steal Login Credentials

Synopsis: A sophisticated phishing campaign masquerades as a targeted organization's technical support team to trick recipients into believing they have emails that have been quarantined and scheduled for deletion. These emails contain a link that leads to the company's legitimate home page; however, the threat actors behind the campaign place an overlay containing a fraudulent login panel over the home page to steal victims' login credentials.

Masquerades as: A notification from an organization's technical support team

Sectors Targeted: All

Motive: To steal victims' organizational account credentials

Threat Actor(s)/Origin: Unknown

Report: [Cofense](#)

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

Phishing mitigation recommendations: The NTIC Cyber Center recommends users remain vigilant for these and other phishing campaigns and be wary of unexpected emails, text messages, and social media messages. Additionally, refrain from clicking on links or opening attachments sent from unknown or untrusted sources and never enable content or macros on Microsoft Office documents before verifying their legitimacy. If you believe you have been infected with malware or have had your login credentials stolen as a result of a phishing campaign, notify your organization's IT security team immediately. To learn how to identify phishing emails, please see the NTIC Cyber Center's product titled [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

New and Notable Malware Campaigns

PyVil Remote Access Trojan

Synopsis: Threat actors created a Python-scripted Remote Access Trojan (RAT), dubbed PyVil RAT, to steal email addresses, passwords, and other sensitive corporate information from financial technology organizations.

Sectors Targeted: Finance

Motive: Profit-Motivated

Threat Actor(s)/Origin: Evilnum

Platforms Affected: Windows

Attack Vector: Spear phishing emails

Associated CVEs: N/A

Mitigation Recommendations: Ensure servers and operating systems are up to date with the latest patches; close any unneeded ports; make sure passwords are lengthy, complex, and unique to each account, and enable multifactor authentication; proactively block IoCs contained in these reports: [Rewterz Threat Alert – Evilnum Targets Financial Sector with Pyvil RAT](#), [Cybereason – No Rest for the Wicked: Evilnum Unleashes PyVil RAT](#).

KryptoCibule Cryptomining Malware

Synopsis: A previously undocumented cryptomining malware variant known as KryptoCibule mines cryptocurrency, hijacks transactions, and steals digital wallets on infected systems.

Sectors Targeted: N/A

Motive: Profit-Motivated

Threat Actor(s)/Origin: Unknown

Platforms Affected: Windows

Attack Vector: Malicious torrent files

Associated CVEs: N/A

Mitigation Recommendations: Refrain from downloading files via torrents and scan all files and systems for malware using reputable antivirus software; ensure servers and operating systems are up to date with the latest patches; monitor networks for suspicious activity; proactively block IoCs contained in ESET's report: [KryptoCibule: The Multitasking Multicurrency Cryptostealer](#).

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

Vulnerabilities

Magento Plugin Magmi

A researcher from Tenable Web Application Security Team [discovered](#) two vulnerabilities ([CVE-2020-5776](#) & [CVE-2020-5777](#)) in the Magmi plugin for Magento online stores that would allow threat actors to conduct remote code execution. CVE-2020-5776 is a cross-site request forgery (CSRF) vulnerability with missing CSRF tokens that would ward off CSRF attacks. CVE-2020-5777 is an authentication bypass vulnerability and allows threat actors to create a denial-of-service (DoS) condition on the Magento database connection. The developers released a new plugin version to fix just the authentication bypass vulnerability. ***The NTIC Cyber Center recommends website administrators of ecommerce stores that use the Magmi plugin to update it to the latest version as soon as possible.***

Data Leaks and Breaches

Warner Music

Music production giant, Warner Music Group, [disclosed](#) a breach affecting some of the company's online stores and its customers' card payment data. Information compromised in the breach includes names, email addresses, payment card data, telephone numbers, billing addresses, and shipping addresses. The breach is attributed to a web skimmer planted on the company's websites that steals customer information. Warner Music Group did not specify which online stores contained the malicious code but is offering free credit monitoring services to customers. Purchases made through PayPal were not affected. ***The NTIC Cyber Center encourages affected Warner Music Group customers consider placing a fraud alert or security freeze on their credit files and activating the free credit monitoring services offered to affected customers and members. Additionally, we recommend website visitors remain vigilant for indications that a webpage may be compromised. These may include being asked twice to enter payment or login information or being prompted for payment card details before being forwarded to a secure payment service provider.***

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



A **dark pattern** is a type of social engineering technique whereby businesses or other organizations use crafty user interface/user experience (UI/UX) designs to manipulate users into making unintended choices. Dark patterns are often used to charge unwitting customers money, maintain a user's attention, harvest personal data, gain or retain subscribers, and display advertisements. While most of these tactics are not necessarily illegal, they can cost customers time, money, and privacy. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

[Average BEC Attempts Are Now \\$80k, but One Group Is Aiming for \\$1.27m per Attack](#)

Analytic Comment: Threat actors behind business email compromise (BEC) scams are attempting to steal \$80,000 on average per attack. This amount has increased compared to Q1 2020 in which the average was \$54,000. One Russia-based BEC threat actor known as Cosmic Lynx demands an average of \$1.27 million per attack. While most BEC threat actors attempt to steal amounts that would not pass thresholds for law enforcement to pursue, Cosmic Lynx surpasses these limits as Russian authorities can protect Russian-based cyber threat actors from US legal repercussions. Since funds may not be recoverable, this highlights the importance of maintaining awareness of BEC scams, refraining from opening attachments or clicking on links within unexpected emails, and verifying financial transaction procedures with multiple parties within your organization before submitting any payment requests received via email or over the phone.

[Ransomware Is a Lurking Threat to US Elections. Here's How.](#)

Analytic Comment: Cybersecurity researchers are concerned that cyber threat actors might use ransomware as a political weapon in the upcoming US presidential election. According to a Cybersecurity and Infrastructure Security Agency (CISA) report, county elections are likely to become a primary target for threat actors looking to disrupt the election process due to the public's need to access the government's election infrastructure. Experts are mostly concerned about undetected attacks compromising voter information, registration statuses, voter eligibility, and resulting in the inability to print ballots or a delay to the check-in process to create confusion, challenging the integrity of the election process. Even though some cyber threat analysts suggest that hackers could not meaningfully manipulate the vote count, it is particularly important that the public maintains confidence in election results and any type of cyber event is enough to create doubt within the election.

Patches and Updates

[Cisco Releases Security Updates](#)
[Mozilla Releases Security Updates for Firefox,](#)
[Firefox ESR, and Thunderbird](#)

ICS-CERT Advisories

[Siemens Industrial Products](#)
[Siemens License Management Utility](#)
[Siemens Polarion Subversion Webclient](#)
[Siemens SIMATIC HMI Products](#)
[Siemens SIMATIC RTLS Locating Manager](#)
[Siemens SIMATIC S7-300 and S7-400 CPUs](#)
[Siemens Siveillance Video Client](#)
[Siemens Spectrum Power](#)
[Siemens UMC Stack \(Update B\)](#)
[Wibu-Systems CodeMeter](#)



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM

Cyber Center

Weekly Cyber Threat Bulletin

17 September 2020
Product No. 2020-09-025
NTIC SIN No. 2.5 | HSEC SIN No. 1

National Capital Region Cyber Threat Spotlight



US Department of Veterans Affairs Suffers Data Breach Affecting over 46,000 Veterans

The US Department of Veterans Affairs (VA) [reported](#) a data breach that compromised the personal information of more than 46,000 veterans. An investigation into the incident revealed that the compromise was a result of unauthorized users gaining access using social engineering methods and exploiting authentication protocols on targeted systems. The VA notified affected individuals, including the next-of-kin of those who are deceased, and is offering free access to credit monitoring services. *The NTIC Cyber Center recommends all affected individuals subscribe to the free credit monitoring services offered and consider placing a fraud alert or security freeze on their credit files with [Equifax](#), [Experian](#), and [TransUnion](#).*

Federal Partner Announcements



CISA
CYBER+INFRASTRUCTURE

Actions to Counter Email-Based Attacks on Election-Related Entities

Malicious cyber actors have been known to use sophisticated phishing operations to target political parties and campaigns, think tanks, civic organizations, and associated individuals. Email systems are the preferred vector for initiating malicious cyber operations.

To protect against these attacks, the Cybersecurity and Infrastructure Security Agency (CISA) has released [CISA Insights: Actions to Counter Email-Based Attacks on Elections-Related Entities](#) in light of [increased sophisticated phishing operations](#) targeting individuals and groups involved in the upcoming U.S. elections.

TLP: WHITE

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

CISA strongly recommends elections-related individuals and organizations to prioritize the protection of email accounts and systems:

- Use provider-offered protections, if utilizing cloud email.
- Secure user accounts on high value services.
- Implement email authentication and other best practices.
- Secure email gateway capabilities.

This latest CISA Insights can be found [here](#).

Other resources are [CISA Security Tip \(ST19-002\): Best Practices for Securing Election Systems](#); [CISA Security Tip \(ST04-014\): Avoiding Social Engineering and Phishing Scams](#); and [Microsoft Blog: New cyberattacks targeting U.S. elections](#).

Iran-Based Threat Actor Exploits VPN Vulnerabilities

CISA and the Federal Bureau of Investigation (FBI) have released a Joint Cybersecurity Advisory on an Iran-based malicious cyber actor targeting several U.S. federal agencies and other U.S.-based networks. This Advisory analyzes the threat actor's indicators of compromise (IOCs); and tactics, techniques, and procedures (TTPs); and exploited Common Vulnerabilities and Exposures (CVEs).

CISA encourages users and administrators to review the following resources for more information.

- [Joint Cybersecurity Advisory: Iran-Based Threat Actor Exploits VPN Vulnerabilities](#)
- [MAR-10297887-1.v1: Iranian Web Shells](#)

Exploit for Netlogon Remote Protocol Vulnerability, CVE-2020-1472

CISA is aware of publicly available exploit code for CVE-2020-1472, an elevation of privilege vulnerability in Microsoft's Netlogon. Although Microsoft provided patches for CVE-2020-1472 in August 2020, unpatched systems will be an attractive target for malicious actors. Attackers could exploit this vulnerability to obtain domain administrator access.

CISA encourages users and administrators to review Microsoft's August Security Advisory for [CVE-2020-1472](#) and [Article](#) for more information and apply the necessary updates.

Current and Emerging Cyber Threats

The Return of Malvertising Campaigns

According to a recent Malwarebytes Labs report, malicious advertising – or malvertising – campaigns are making a return as a viable delivery mechanism for threat actors looking to deploy malware to unsuspecting users who continue to use vulnerable web browsers such as Internet Explorer. After noticing a spike in malvertising activity, researchers discovered one of the largest malvertising campaigns in which threat actors exploited the advertising networks on almost every website hosting adult content as well as on a website of a top publisher. These threat actors exploited the vulnerabilities within Internet Explorer ([CVE-2019-0752](#)) and Flash Player ([CVE-2018-15982](#)) with redirection pages that infected

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

systems with the ZLoader and Raccoon information-stealing malware variants. *The NTIC Cyber Center recommends all users discontinue the use of vulnerable and unsupported web browsers such as Internet Explorer and consider using a reputable ad-blocker to protect systems against malvertising campaigns. We also recommend always running reputable antivirus software and keeping it up to date with the latest virus definitions. Network administrators are encouraged to proactively block the indicators of compromise (IoCs) provided in the Malwarebytes Labs [report](#).*

Magento Ecommerce Platform Impacted by Large Automated Attack

A hack that [compromised](#) the credit card information of approximately 2,000 online stores is now known as the largest successful automated cyber-attack against the Magento ecommerce platform. The threat actors behind this campaign have deployed malicious JavaScript onto Magento websites to steal the credit card information from website visitors as they enter it in the checkout portion of the online transaction. It is reported that majority of the compromised websites were running Magento 1, a vulnerable and unsupported version of the platform. *The NTIC Cyber Center recommends that website administrators of online stores running Magento 1 update the platform to the more secure Magento 2 as soon as possible and change all administrative passwords to help reduce additional exploitation and data theft.*



Phishing Attack Abuses Amazon Simple Email Service and Uses Real-Time Validation Technique

Synopsis: ArmorBlox researchers provide an overview on the attack flow of an advanced Microsoft Office 365 phishing attack that abuses the Amazon Simple Email Service and uses a real-time validation technique on Active Directory to steal users' login credentials.

Masquerades as: financial reports

Sectors Targeted: All

Motive: Credential theft

Threat Actor(s)/Origin: Unknown

Platforms Affected: Amazon Simple Email Service, Microsoft Active Directory and Office 365

Report: [Armorblox](#)

Phishing Campaign Masquerades as Phishing Training Reminder

Synopsis: Researchers discovered a new phishing campaign that spoofs phishing training reminder emails from cybersecurity firm KnowBe4 to trick recipients into divulging their email account login credentials.

Masquerades as: KnowBe4 phishing training notification emails

Sectors Targeted: All

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER**Motive:** Credential theft**Threat Actor(s)/Origin:** Unknown**Platforms Affected:** Microsoft Outlook**Report:** [KnowBe4](#)

Phishing mitigation recommendations: The NTIC Cyber Center recommends users remain vigilant for these and other phishing campaigns and be wary of unexpected emails, text messages, and social media messages. Additionally, refrain from clicking on links or opening attachments sent from unknown or untrusted sources and never enable content or macros on Microsoft Office documents before verifying their legitimacy. If you believe you have been infected with malware or have had your login credentials stolen as a result of a phishing campaign, notify your organization's IT security team immediately. To learn how to identify phishing emails, please see the NTIC Cyber Center's product titled [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

New and Notable Malware Campaigns

The Return of the Dridex Trojan

Synopsis: Researchers recently discovered that the Cutwail botnet resumed delivery of the Dridex Trojan to victims via malicious email campaigns.

Sectors Targeted: All**Motive:** Profit-motivated; banking credential theft**Threat Actor(s)/Origin:** Unknown**Platforms Affected:** Windows**Attack Vector:** Phishing emails containing malicious Excel attachments**Mitigation Recommendations:** Disable macros by default; run reputable and updated antivirus software on all endpoints; proactively block IoCs contained in the SANS ISC report titled [Recent Dridex Activity](#).

Data Leaks and Breaches

Staples

The office supply company Staples [experienced](#) a data breach in which threat actors accessed what the company classified as "non-sensitive" data from customers' orders. The compromised data includes names, addresses, email addresses, phone numbers, the last four digits of payment card numbers, and details about the order including the delivery, cost, and what product was purchased. Threat actors can use this information to conduct phishing and phone call scams. *The NTIC Cyber Center recommends that affected Staples customers remain vigilant for phishing campaigns that result from this breach, change any passwords associated with their account, and continuously monitor accounts for any unauthorized or suspicious activity.*

Artech

US staffing company Artech [disclosed](#) a data breach resulting from a Sodinokibi/REvil ransomware attack that occurred in January 2020. Reportedly, the attackers exploited the Pulse Secure VPN vulnerability [CVE-2019-11510](#) to gain access to the company's systems. The stolen data includes names, Social Security numbers, medical information, health insurance information, financial information, payment card information, driver's license/state identification numbers, government-issued identification

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

numbers, passport numbers, visa numbers, electronic/digital signatures, usernames, and passwords. Artech sent a data breach notice to victims. ***The NTIC Cyber Center recommends all affected individuals monitor their financial and other associated accounts for unauthorized or suspicious activity, change their Artech passwords, enable multifactor authentication on every account that offers it, and consider placing a fraud alert or security freeze on their credit files with [Equifax](#), [Experian](#), and [TransUnion](#). We also recommend all administrators of vulnerable Pulse VPN servers apply the vendor-supplied patch as soon as possible. To help identify vulnerable instances within network environments, CISA has provided a free tool, available via GitHub, [here](#).***

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



Car warranty scams are profit-motivated social engineering schemes designed to trick unsuspecting car owners into purchasing an extended warranty or service contract for their vehicles. The companies behind these scams bombard vehicle owners with robocalls, emails, text messages, and physical mail such as postcards and official-looking notices that claim the vehicle's warranty is about to expire. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

[Ransomware Accounted for 41 Percent of All Cyber Insurance Claims in H1 2020](#)

Analytic Comment: According to cyber insurance firm Coalition, ransomware attacks accounted for 41 percent of all cyber insurance claims filed in the first half of 2020. Among their policyholders, the company observed a 206 percent increase in the frequency of ransomware attacks and noted that the average ransom demand increased by 47 percent. The findings in this report highlight the increasing threat that ransomware poses to organizations and emphasizes the importance of having a robust cyber incident response plan in place prior to a cyber incident occurring. To download a copy of the NTIC Cyber Center Guide for Cyber Incident Response Planning and the Ransomware Mitigation Guide, please visit our website [here](#).

[Managed IT Providers: The Cyber-Threat Actors' Gateway to SMBs](#)

Analytic Comment: The use of managed service providers (MSPs) can pose a significant cyber risk to small and medium-sized businesses (SMBs) as cyber threat actors seek to impact as many organizations as they can. Unfortunately, a vulnerable or compromised MSP can serve as the single point of failure for all of their clients, potentially resulting in severe financial and reputational loss. This is why it is crucial for both MSPs and SMBs to take effective steps in reducing their cyber risk and regularly auditing access controls to limit the impact of a potential compromise.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

<u>Patches and Updates</u>	<u>ICS-CERT Advisories</u>
Adobe Releases Security Update for Media Encoder	AVEVA Enterprise Data Management Web ENTTEC Lighting Controllers (Update A) FATEK Automation PLC WinProladder HMS Networks Ewon Flexy and Cosy Philips Patient Monitoring Devices



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM

Cyber Center

Weekly Cyber Threat Bulletin

24 September 2020
Product No. 2020-09-034
NTIC SIN No. 2.5 | HSEC SIN No. 1

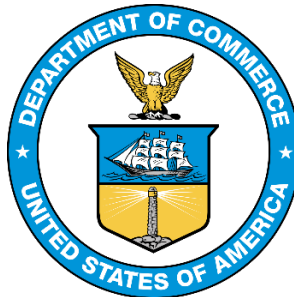
National Capital Region Cyber Threat Spotlight



APT28/Fancy Bear Uses NATO Theme to Deliver Zebrocy Malware

The Russian hacking group APT28, also known as Fancy Bear, is targeting government organizations using a phishing campaign that attempts to infect victims with a strain of Zebrocy Delphi malware. Researchers from Quo Intelligence first detected this campaign on August 9, 2020 and discovered that it used upcoming NATO training information as a lure, targeting a government organization in Azerbaijan and possibly other NATO members and countries involved in NATO exercises. At the time of discovery, the command-and-control (C2) infrastructure used to conduct the campaign was active and hosted in France; however, French authorities have since dismantled it. The phishing emails associated with this campaign attempt to deliver a ZIP file labeled "Course 5 – 16 October 2020". If decompressed using the WinRAR utility, the ZIP file drops two files, one of which contains Zebrocy, a Trojan written in the Go programming language and designed to steal information from and drop additional malware onto infected systems. APT28 has used Zebrocy in previous campaigns to target government organizations across the globe. *The NTIC Cyber Center recommends all network administrators review the Quo Intelligence report titled [APT28 Delivers Zebrocy Malware Campaign Using NATO Theme as Lure](#) and block the associated indicators of compromise (IoCs).*

Federal Partner Announcements



TLP: WHITE

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States

In response to President Trump's Executive Orders signed August 6, 2020, the Department of Commerce (Commerce) on September 18, 2020 announced prohibitions on transactions relating to mobile applications (apps) WeChat and TikTok to safeguard the national security of the United States. The Chinese Communist Party (CCP) has demonstrated the means and motives to use these apps to threaten the national security, foreign policy, and the economy of the US. Today's announced prohibitions, when combined, protect users in the U.S. by eliminating access to these applications and significantly reducing their functionality.

"Today's actions prove once again that President Trump will do everything in his power to guarantee our national security and protect Americans from the threats of the Chinese Communist Party," said U. Department of Commerce Secretary Wilbur Ross. "At the President's direction, we have taken significant action to combat China's malicious collection of American citizens' personal data, while promoting our national values, democratic rules-based norms, and aggressive enforcement of US laws and regulations."

While the threats posed by WeChat and TikTok are not identical, they are similar. Each collects vast swaths of data from users, including network activity, location data, and browsing and search histories. Each is an active participant in China's civil-military fusion and is subject to mandatory cooperation with the intelligence services of the CCP. This combination results in the use of WeChat and TikTok creating unacceptable risks to our national security.

As of September 20, 2020, the following transactions are prohibited:

1. Any provision of service to distribute or maintain the WeChat or TikTok mobile applications, constituent code, or application updates through an online mobile application store in the US;
2. Any provision of services through the WeChat mobile application for the purpose of transferring funds or processing payments within the U.S.

As of September 20, 2020, for WeChat and as of November 12, 2020, for TikTok, the following transactions are prohibited:

1. Any provision of internet hosting services enabling the functioning or optimization of the mobile application in the US;
2. Any provision of content delivery network services enabling the functioning or optimization of the mobile application in the US;
3. Any provision directly contracted or arranged internet transit or peering services enabling the function or optimization of the mobile application within the US;
4. Any utilization of the mobile application's constituent code, functions, or services in the functioning of software or services developed and/or accessible within the US.

Any other prohibitive transaction relating to WeChat or TikTok may be identified at a future date. Should the U.S. Government determine that WeChat's or TikTok's illicit behavior is being replicated by another app somehow outside the scope of these executive orders, the President has the authority to consider whether additional orders may be appropriate to address such activities. The President has provided until November 12 for the national security concerns posed by TikTok to be resolved. If they are, the prohibitions in this order may be lifted.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER**CISA Releases Alert on LokiBot Malware**

The Cybersecurity and Infrastructure Security Agency (CISA) has observed a notable increase in the use of LokiBot malware by malicious cyber actors since July 2020. Throughout this period, CISA's EINSTEIN Intrusion Detection System, which protects federal, civilian executive branch networks, has detected persistent malicious LokiBot activity. LokiBot uses a credential- and information-stealing malware, often sent as a malicious attachment and known for being simple, yet effective, making it an attractive tool for a broad range of cyber actors across a wide variety of data compromise use cases. For more information, including technical details, IoCs, and mitigation recommendations, please see CISA [Alert AA20-266A](#).

Current and Emerging Cyber Threats**Threat Actors Use Hexadecimal-Encoded IP Addresses to Bypass Security Filters**

Researchers have recently discovered a spam email campaign using IP addresses coded in a hexadecimal format to bypass email security filters. In this specific campaign, the URLs embedded in the body of the emails contain hexadecimal-encoded IP addresses that redirect victims to fraudulent pharmaceutical websites. These websites contain marketing videos and testimonials to lure victims into purchasing fake pills, medicine, and healthcare products. It is reported that these fraudulent pharmaceutical websites are hosted on domains that have been recently purchased, suggesting that this is a new campaign. *The NTIC Cyber Center recommends users remain vigilant for spam email campaigns, avoid clicking unexpected emails, and refrain from clicking on links from unknown or untrusted sources. IoCs associated with this campaign are available in Trustwave's [report](#).*

**Texas Vendor Targeted in Profit-Motivated Phishing Campaign**

Synopsis: A phishing campaign spoofed a state government agency to defraud a private electronics vendor out of goods such as laptops and hard drives.

Masquerades as: A government agency sending a "request for quotation" to vendors

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER**Sectors Targeted:** Private sector vendors**Motive:** Profit-motivated**Threat Actor(s)/Origin:** Unknown**Platforms Affected:** Microsoft Office 365**Report:** [Abnormal Security](#)

Phishing mitigation recommendations: The NTIC Cyber Center recommends users remain vigilant for these and other phishing campaigns and be wary of unexpected emails, text messages, and social media messages. Additionally, refrain from clicking on links or opening attachments sent from unknown or untrusted sources and never enable content or macros on Microsoft Office documents before verifying their legitimacy. If you believe you have been infected with malware or have had your login credentials stolen as a result of a phishing campaign, notify your organization's IT security team immediately. To learn how to identify phishing emails, please see the NTIC Cyber Center's product titled [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

New and Notable Malware Campaigns

MrbMiner Targets MSSQL Servers

Synopsis: Threat actors use brute-force password attacks on Microsoft SQL (MSSQL) servers to compromise and install a new cryptomining malware dubbed MrbMiner.

Sectors Targeted: All**Motive:** Profit-motivated**Threat Actor(s)/Origin:** MrbMine**Platforms Affected:** MSSQL servers**Attack Vector:** Brute-force attacks on MSSQL servers**Report:** [ZDNet](#)

Mitigation Recommendations: Regularly audit networks for vulnerable and unsecured servers and devices and ensure that all running software is patched with the latest version. Replace default usernames with something unique, make sure passwords are lengthy, complex, and unique to each account, and enable multifactor authentication.

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data and organization at risk. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

Maze Ransomware Operators Use Virtual Machines to Encrypt Data

Maze ransomware operators are now using virtual machines (VMs) to bypass security measures and encrypt data on a targeted system. In one cyber incident noted by Sophos researchers, after Maze ransomware operators were unable to execute the ransomware on the compromised system, they deployed an MSI file that installed the VirtualBox VM software and a customized Windows 7 VM. The VM then mounted the host system's drives as remote shares and launched the ransomware in the VM to encrypt the

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

shares' files. Use of the VM allows the attack to remain undetected by any security software running on the host system. This incident highlights how ransomware operators are adapting increasingly sophisticated techniques to execute successful attacks against victims. More information about this technique, including IoCs, is available in the Sophos report titled [Maze Attackers Adopt Ragnar Locker Virtual Machine Technique](#).

Ransomware Attack Contributed to the Death of a Hospital Patient in Germany

A ransomware attack on the University Hospital Düsseldorf (UKD) in Germany [resulted](#) in the death of a patient who had to be transported to a hospital that was further away due to the impact on UKD's emergency care. The attackers exploited [CVE-2019-19781](#), a vulnerability present within unpatched Citrix appliances. The ransom note discovered on UKD's servers was addressed to Heinrich Heine University and not to the hospital itself, prompting German law enforcement to contact the ransomware operators and explain that their target was a hospital and not the university. The threat actors behind this attack withdrew their demands and provided the hospital with the decryption key free of charge.

Vulnerabilities

Security Concerns Associated with US 2020 Presidential Mobile Apps

Researchers have discovered several security concerns [surrounding](#) mobile applications associated with the upcoming US presidential election. The "Vote Joe" app, promoted by the Biden 2020 presidential campaign to engage with potential voters, reportedly leaks sensitive information such as voters' political affiliations and previous voting decisions and shares this data with an intelligence service designed to predict users' voting choices. The app also collects information from users' contact lists, as outlined in its terms of service. Researchers discovered that the official Trump 2020 presidential campaign app also collects a large amount of user data and, in June, the APK file for the Android version of the app exposed hardcoded secret keys associated with Twitter and Google services. ***The NTIC Cyber Center recommends all mobile device users carefully read apps' terms of service prior to installation and carefully scrutinize all permissions requested by the app. If the requested permissions do not match the functionality of the app, refrain from installing it. We strongly encourage users to refrain from allowing apps to access your contacts' data to protect their privacy and information.***

BLESA Bluetooth Vulnerability

Billions of mobile phones, tablets, laptops, and Internet-of-Things (IoT) devices are [reportedly](#) vulnerable to a new vulnerability named BLESA, an acronym for Bluetooth Low Energy Spoofing Attack. BLESA impacts any device running the Bluetooth Low Energy (BLE) protocol, which is designed to conserve battery power in devices maintaining Bluetooth connections. The vulnerability resides within the Bluetooth reconnection process as the authentication protocol when establishing a connection to another device is not mandatory and could be circumvented by an attacker. There is currently no patch available. ***The NTIC Cyber Center recommends pairing devices via a Bluetooth connection in controlled environments and turning off Bluetooth connections on devices unless needed.***

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

Data Leaks and Breaches



Fitness center chain Town Sports International, owner of New York Sports Clubs, Boston Sports Clubs, Philadelphia Sports Clubs, Washington Sports Clubs, Lucille Roberts, and Total Woman Gym and Spa, [suffered](#) a data leak that potentially exposed the personal data of over 600,000 members and staff. Exposed data includes names, addresses, phone numbers, email addresses, payment card information, and billing histories. ***The NTIC Cyber Center recommends members of any of the aforementioned fitness centers maintain awareness for phishing campaigns resulting from this data exposure and monitor financial accounts for suspicious or unauthorized activity.***

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



Government grant scams are a type of social engineering scheme in which perpetrators use the promise of grant funding to steal money and/or elicit personally identifiable information (PII). Scammers notify victims that they qualify for government grants, requesting a fee to process the grant. If victims pay, the perpetrators will either flee with the money or request additional payments, citing unforeseen circumstances or complications. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

[Researchers Identify the Departments and Industries Most Susceptible to Email-Based Cyber Attacks](#)

Analytic Comment: Recent studies indicate that phishing remains one of the top threats to organizations. In a Keepnet Labs phishing simulation exercise, recipients opened the mock phishing email 50 percent of the time, clicked on an attachment or link in the email 32 percent of the time, and divulge their personal or sensitive information 13 percent of the time. This study also determined that employees within consulting firms and the finance, telecommunications, and transportation sectors are the most likely to open a phishing email. This highlights the importance of conducting regular phishing awareness training for all employees and employing a reputable email security gateway to reduce the number of malicious emails that reach users' inboxes.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

Patches and Updates

[Adobe Releases Security Update for Media Encoder](#)
[Apple Releases Security Updates](#)
[Drupal Releases Security Updates](#)
[Google Releases Security Updates for Chrome](#)
[Mozilla Releases Security Updates for Firefox and Firefox ESR](#)
[Samba Releases Security Update for CVE-2020-1472](#)

ICS-CERT Advisories

[Advantech WebAccess Node](#)
[GE Digital APM Classic](#)
[GE Reason S20 Ethernet Switch](#)
[Philips Clinical Collaboration Platform](#)
[Wibu-Systems CodeMeter \(Update A\)](#)



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM

Cyber Center

Weekly Cyber Threat Bulletin

1 October 2020
Product No. 2020-10-001
NTIC SIN No. 2.5 | HSEC SIN No. 1

National Capital Region Cyber Threat Spotlight



Emotet Remains a Top Security Concern across the Globe

Microsoft Security Intelligence posted a number of [tweets](#) detailing a recent [outbreak](#) of Emotet activity that noticeably surpassed any other currently active malware operations. These campaigns distribute malicious emails containing PDF file attachments with a link that directs victims to a malicious executable file. If downloaded, Emotet will infect the device and turn it into a bot to be used in future attacks, sold to other threat groups, or used in ransomware attacks. France, Japan, New Zealand, Italy, and the Netherlands have reported a surge of Emotet-laden emails and have coordinated cyber threat intelligence sharing efforts to release alerts on campaigns to organizations within their respective countries. ***The NTIC Cyber Center recommends users remain vigilant for Emotet email campaigns, avoid opening unexpected emails, and refrain from clicking on links or opening attachments from unknown or untrusted sources. If you believe you have been infected with Emotet, notify your organization's IT security team immediately so they may contain and remediate the infection.***

Federal Partner Announcements



CISA
CYBER+INFRASTRUCTURE

October Is National Cybersecurity Awareness Month

Now in its 17th year, National Cybersecurity Awareness Month (NCSAM) continues to raise awareness about the importance of cybersecurity across our Nation, ensuring that all Americans have the resources they need to be safer and more secure online.

NCSAM Theme and Schedule

CISA and the [National Cyber Security Alliance \(NCSA\)](#) are proud to announce this year's theme:

"Do Your Part. #BeCyberSmart."

TLP: WHITE

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

This theme encourages individuals and organizations to own their role in protecting their part of cyberspace, stressing personal accountability and the importance of taking proactive steps to enhance cybersecurity.

NCSAM emphasizes “If You Connect It, Protect It.” Throughout October, CISA and NCSA will focus on the following areas in our promotions and outreach:

- October 1 and 2: Official NCSAM Kick-off
- Week of October 5 (Week 1): If You Connect It, Protect It
- Week of October 12 (Week 2): Securing Devices at Home and Work
- Week of October 19 (Week 3): Securing Internet-Connected Devices in Healthcare
- Week of October 26 (Week 4): The Future of Connected Devices

Use NCSAM’s hashtag #BeCyberSmart before and during October to promote your involvement in raising cybersecurity awareness.

For more NCSAM resources, please visit CISA’s [website](#).

CISA and MS-ISAC Release Ransomware Guide

The Cybersecurity and Infrastructure Security Agency (CISA) and the [Multi-State Information Sharing & Analysis Center](#) (MS-ISAC) have released a joint [Ransomware Guide](#) that details practices that organizations should continuously engage in to help manage the risk posed by ransomware and other cyber threats. The in-depth guide provides actionable best practices for ransomware prevention as well as a ransomware response checklist that can serve as a ransomware-specific addendum to organization cyber incident response plans.

CISA encourages users and administrators to review the [Ransomware Guide](#) and CISA’s [Ransomware webpage](#) for additional information.

Current and Emerging Cyber Threats

Palmerworm Cyber-Espionage Group Targets Multiple Sectors

Symantec researchers recently discovered a new Palmerworm cyber espionage campaign targeting media, construction, engineering, electronics, and finance organizations in the US, Japan, Taiwan, and China. The attacks they observed began in August 2019 and continued throughout 2020. Palmerworm uses custom malware, dual-use tools, and living-off-the-land techniques to target and install backdoors onto victims’ networks and steal data. Some of the legitimate tools used in these attacks include Putty, PSEXec, SNScan, and WinRAR. Although no official attribution has been made, Taiwanese officials [believe](#) that this group is affiliated with the Chinese government. ***The NTIC Cyber Center recommends all network administrators proactively block the associated indicators of compromise (IoCs) contained in Symantec’s report titled [Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors](#).***

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data and organization at risk. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

AgeLocker Ransomware Targets QNAP NAS Storage Devices

A ransomware campaign is actively [targeting](#) QNAP Network Attached Storage (NAS) devices with AgeLocker ransomware to lock and steal victim files. AgeLocker uses an encryption algorithm called Age (Actually Good Encryption) to takeover GPG (GNU Privacy Guard) that encrypts files, backups, and streams. On a compromised system, AgeLocker adds a text header that starts with the URL “age-encryption[.]jorg” to each encrypted file. It is currently unknown how these threat actors are gaining access to their victims’ devices but, after encryption process is finished, victims are left with a .txt file containing instructions on how to submit the ransom payment and obtain the decryption tool. There is currently no publicly available decryption tool for this variant.

Mount Locker Ransomware Demands Millions

Mount Locker is a ransomware [campaign](#) that targets corporate networks and demands multi-million dollar ransoms after stealing and encrypting victims' files. The threat actors behind Mount Locker threaten to publish the stolen data of victims who do not remit payment. Analysis of the Mount Locker ransomware variant reveals that it uses ChaCha20 to encrypt files and the RSA-2048 public key to encrypt the encryption key. The ransom note contains instructions on how to access a Tor site to correspond with the ransomware operators via a web chat service to ask questions and negotiate the ransom. There is currently no publicly available decryption tool for this variant.



Apple Smishing Campaign Targets Credit Card Data

Synopsis: Researchers at Sophos uncovered an Apple smishing (SMS phishing) campaign that distributes fraudulent text messages to steal credit card data.

Masquerades as: An Apple chatbot

Sectors Targeted: All

Motive: Profit-motivated

Threat Actor(s)/Origin: Unknown

Platforms Affected: iOS

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER**Report:** [Sophos](#)

Phishing mitigation recommendations: The NTIC Cyber Center recommends users remain vigilant for these and other phishing campaigns and be wary of unexpected emails, text messages, and social media messages. Additionally, refrain from clicking on links or opening attachments sent from unknown or untrusted sources and never enable content or macros on Microsoft Office documents before verifying their legitimacy. If you believe you have been infected with malware or have had your login credentials stolen as a result of a phishing campaign, notify your organization's IT security team immediately. To learn how to identify phishing emails, please see the NTIC Cyber Center's product titled [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

New and Notable Malware Campaigns

Alien – A New Password-Stealing Malware Targeting Android Devices

Synopsis: Over 200 Android applications are vulnerable to a new password stealing malware named Alien that is targeting banking applications. This malware infestation also presents phishing pages designed to steal login credentials for popular social media platforms, instant messaging applications, and cryptocurrency applications while also bypassing some multi-factor authentication (MFA) codes generated by authenticator applications.

Sectors Targeted: All

Motive: Steals login credentials for banking apps, social media platforms, instant messaging apps, and cryptocurrency apps

Threat Actor(s)/Origin: Unknown

Platforms Affected: Android

Attack Vector: Malicious Android applications

Mitigation Recommendations: Only download applications from trusted and vetted sources, keep device operating systems up to date, backup data on mobile devices regularly, refrain from clicking on links from unknown or untrusted sources, and scrutinize unexpected links sent via text message. Enable MFA on any account that offers it to reduce the risk of compromise resulting from stolen login credentials. Users who suspect that their devices have been compromised should perform a factory reset and restore devices to manufacturer default settings and are strongly encouraged to change their account credentials and monitor accounts for suspicious or unauthorized activity. For a list of affected applications, please see the Threat Fabric report titled [Alien – The Story of Cerberus' Demise](#).

Joker Malware Continues to Target Android Devices

Synopsis: Joker malware, embedded in several malicious apps, was discovered in the official Google Play store. It bypasses the Google Play vetting process by changing its code, changing execution methods, and modifying its payload-retrieving techniques.

Sectors Targeted: All

Motive: Data theft, billing fraud

Threat Actor(s)/Origin: Unknown

Platforms Affected: Android

Attack Vector: Malicious Android applications

Mitigation Recommendations: Thoroughly research apps before downloading them and only install trusted and vetted apps. If the permissions required do not match the advertised functionality of the app, do not install it. After installing any new app, monitor the device for unusual behavior such as excessive

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

power consumption, excessive data usage, unexpected pop-ups, and uninstall problematic apps immediately, performing a factory reset of the device if necessary. For a list of recent malicious apps and more information, please see the ZScaler report titled [Joker Playing Hide-and-Seek with Google Play](#).

Taidoor RAT

Synopsis: Taidoor is a remote access trojan (RAT) developed and used by Chinese nation-state actors to create backdoors in targeted networks. It is comprised of a loader and a RAT module and establishes connections with command-and-control (C2) servers controlled by the attackers.

Sectors Targeted: Governments, corporations, think tanks, healthcare

Motive: Data theft, espionage

Threat Actor(s)/Origin: Chinese nation-state actors

Platforms Affected: Windows

Attack Vector: Spear phishing campaigns

Mitigation Recommendations: Refrain from clicking on links or opening attachments sent from unknown or untrusted sources and never enable content or macros on Microsoft Office documents before verifying their legitimacy. Network administrators are encouraged to review CISA's Malware Analysis Report [AR20-216A](#) and proactively block the associated IoCs provided in this and the ReversingLabs report titled [Taidoor – A Truly Persistent Threat](#).

LodaRAT

Synopsis: Cisco Talos researchers recently discovered new versions of LodaRAT, a remote access trojan written in AutoIt, used in attacks against victims. These versions contain additional functions including a hex-encoded PowerShell keylogger script and a Visual Basic (VB) script.

Sectors Targeted: All

Motive: Data theft, espionage

Threat Actor(s)/Origin: Unknown

Platforms Affected: Windows

Attack Vector: Malicious email attachments

Mitigation Recommendations: Refrain from clicking on links or opening attachments sent from unknown or untrusted sources and never enable content or macros on Microsoft Office documents before verifying their legitimacy. Network administrators are encouraged to proactively block the associated IoCs provided in the Cisco Talos report titled [LodaRAT Update: Alive and Well](#).

Data Leaks and Breaches



Shopify Inc. [disclosed](#) a data breach that resulted in the exposure of data associated with approximately 200 merchants. The breach is attributed to two rogue employees who stole customer transaction records from some of these merchants. Information exposed in the data breach may include customers' names, mailing addresses, email addresses, and order details. Shopify does not currently believe that full payment card numbers and financial information were compromised. Shopify immediately terminated the rogue employees and is working with law enforcement in an investigation of the incident and is working to

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

remediate the issue. *The NTIC Cyber Center recommends that affected Shopify merchants and customers remain vigilant for phishing campaigns that may result from this breach, change any passwords associated with their account, and continuously monitor accounts for any unauthorized or suspicious activity.*

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



Like-farming, also known as **like-harvesting**, is a social engineering technique that fraudsters employ to increase online engagement and boost the popularity of social media posts and pages. Those who use this method – known as like-farmers – create new social media pages and use them to post images, popular quotes, or memes designed to garner attention from social media users by encouraging them to “like” and “share” the posts to their personal pages. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

[All Four of the World's Largest Shipping Companies Have Now Been Hit by Cyber-Attacks](#)

Analytic Comment: Container shipping company CMA CGM experienced a ransomware attack on September 28, 2020, making it one of four of the largest maritime shipping companies in the world to have been hit by ransomware in four years. Researchers have noticed a surge in attacks targeting ships with ransomware, USB malware, and worms discovered on the ship's information technology systems, highlighting the industries need to focus on securing their technical infrastructure. The companies within this industry have experienced their most critical attacks not on boats but on their shore-based networks that contain personnel information, ship management systems, and container transport records. This underscores the need for the shipping industry to allocate more resources to cybersecurity, especially to protect shore-based systems.

[DDoS Attacks Are Getting More Powerful as Attackers Change Tactics](#)

Analytic Comment: Distributed Denial of Service (DDoS) attacks have been more frequent and more disruptive this year. Research suggests that compared to last year, there has been a 15 percent increase in DDoS attacks. Additionally, the size and potency of the strongest attacks increased 2,851 percent since 2017. This, coupled with the fact that the source code to conduct these attacks are often available for free, allows threat actors to conduct severe DDoS attacks at unprecedented rates. Since organizations are more likely than ever to experience a DDoS attack, it is imperative that they take steps to prevent and mitigate this threat as soon as possible.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

Patches and Updates

[Apple Releases Security Updates](#)
[Cisco Releases Security Updates for Multiple
Products](#)
[Mozilla Releases Security Updates for Firefox
and Firefox ESR](#)

ICS-CERT Advisories

[3S CoDeSys \(Update A\)](#)
[B&R Automation SiteManager and
GateManager](#)
[GE Digital APM Classic](#)
[GE Reason S20 Ethernet Switch](#)
[MB Connect line mbCONNECT24,
mymbCONNECT24](#)
[Yokogawa WideField3](#)



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM

Cyber Center

Weekly Cyber Threat Bulletin

8 October 2020
Product No. 2020-10-010
NTIC SIN No. 2.5 | HSEC SIN No. 1

National Capital Region Cyber Threat Spotlight



Iranian Cyber-Espionage Group MuddyWater Using ZeroLogon Exploits in Attacks

Microsoft recently issued a [warning](#) to Windows users about MuddyWater, also known as MERCURY and SeedWorm, an Iranian state-sponsored cyber-espionage group using exploiting the Zerologon vulnerability ([CVE-2020-1472](#)) in several attacks over the past two weeks. CVE-2020-1472 is a critical 10/10 vulnerability that, if exploited, allows attackers to elevate their privileges to that of a domain administrator and successfully control a domain. Microsoft released a security update for affected systems and guidance associated with this vulnerability on August 11, 2020. *The NTIC Cyber Center recommends all network administrators prioritize mitigating this vulnerability and review the following guidance from Microsoft:*

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472>

<https://support.microsoft.com/en-us/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc>

Federal Partner Announcements



CISA
CYBER+INFRASTRUCTURE

CISA Releases Telework Essentials Toolkit

The Cybersecurity and Infrastructure Security Agency (CISA) has released the [Telework Essentials Toolkit](#), a comprehensive resource of telework best practices. The Toolkit provides three personalized modules for executive leaders, IT professionals, and teleworkers. Each module outlines distinctive

TLP: WHITE

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

TLP: WHITE
NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

security considerations appropriate for their role:

- Actions for executive leaders that drive cybersecurity strategy, investment and culture
- Actions for IT professionals that develop security awareness and vigilance
- Actions for teleworkers to develop their home network security awareness and vigilance

CISA encourages users and administrators to review the [Telework Essentials Toolkit](#) and the [CISA Telework](#) page for more information.

CISA Releases Election Disinformation Toolkit

To ensure state and local election officials have the tools to actively communicate timely, trusted, and verified election process details and mitigate against potential impacts of false or misleading information, CISA has released an [Election Disinformation Toolkit](#).

The Toolkit includes talking points and frequently asked questions that can help election officials communicate their role as “trusted voices” for election information. Core messaging in the Toolkit emphasizes that “we’re all in this together” and that election officials can help citizens avoid contributing to the spread of disinformation.

To view the Election Disinformation Toolkit, or to learn more about CISA’s effort to enhance the integrity and resilience of the Nation’s election infrastructure and accuracy of the free and fair elections, please visit [CISA.gov/protect2020](https://cisa.gov/protect2020).

CISA and MS-ISAC Release Activity Alert on Emotet Malware

CISA has released an Activity Alert (TLP:WHITE) [AA20-280A: Emotet Malware](#) written by CISA and Multi-State Information Sharing & Analysis Center (MS-ISAC).

Emotet—a sophisticated Trojan commonly functioning as a downloader or dropper of other malware—resurfaced in July 2020, after a dormant period that began in February. Since August, CISA and MS-ISAC have seen a significant increase in malicious cyber actors targeting state and local governments with Emotet phishing emails. This increase has rendered Emotet one of the most prevalent ongoing threats, especially for state, local, tribal, and territorial (SLTT) governments.

Technical Details Include:

Emotet is an advanced Trojan primarily spread via phishing email attachments and links that, once clicked, launch the payload. The malware then attempts to proliferate within a network by brute forcing user credentials and writing to shared drives. Emotet is difficult to combat because of its “worm-like” features that enable network-wide infections. Additionally, Emotet uses modular Dynamic Link Libraries to continuously evolve and update its capabilities.

To secure against Emotet, CISA and MS-ISAC recommend:

- Implementing the mitigation measures described in this Alert, which include applying measures to block suspicious attachments, using antivirus software, and blocking suspicious IPs.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER**CISA and CNMF Identify a new Malware Variant - SLOTHFULMEDIA**

The Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Defense (DOD) Cyber National Mission Force (CNMF) have identified a malware variant—referred to as SLOTHFULMEDIA—used by a sophisticated cyber actor. In addition, U.S. Cyber Command has released the malware sample to the malware aggregation tool and repository, VirusTotal.

CISA encourages users and administrators to review Malware Analysis Report [MAR-10303705-1.v1](#) and U.S. Cyber Command's [VirusTotal](#) page for more information.

Current and Emerging Cyber Threats**Attackers Abuse Paste Sites to Store and Deliver Malicious Code**

Researchers at Juniper Threat Labs identified multiple threat campaigns that use an online text storage website, or paste site, to deliver malware to victims. Paste sites are online content hosting services that visitors can use to store plain text and are often used by software developers to share code. However, attackers can abuse these sites to post and store malicious code. In the attacks that Juniper observed, attackers stored malicious code on paste sites and then sent phishing emails with malicious attachments that, if opened, downloaded this code and executed it on the victim's system. Researchers have observed attackers using this method to infect victims with Agent Tesla, W3Cryptolocker ransomware, Redline Stealer, and LimeRAT malware. *The NTIC Cyber Center recommends all network administrators review Juniper's report titled [New Pastebin-Like Service Used in Multiple Malware Campaigns](#) and block the associated indicators of compromise (IoCs).*

**Phishing Campaign Uses President Trump's Health as Lure to Deliver BazarLoader**

Synopsis: Cybersecurity firm Proofpoint discovered a phishing campaign promising to deliver information about President Trump's health that infects victims with BazarLoader, a trojan that creates a backdoor into networks.

Masquerades as: Emails containing information about President Trump's health

Sectors Targeted: All

Motive: BazarLoader malware delivery, network compromise

Threat Actor(s)/Origin: Unknown

Platforms Affected: Windows

Report: [BleepingComputer](#)

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER**Spam Campaign Adds Random Text to Shortened URLs to Avoid Detection**

Synopsis: Researchers observed spam campaigns in which threat actors inject random text into generated shortened URL links of legitimate URL links to evade human and spam filter detection. This new technique uses phishing emails to deliver a malicious Windows PowerPoint executable file named “mshta.exe” that will prompt the recipient to enable macros. If enabled, LokiBot malware will download onto the compromised device.

Masquerades as: Shortened legitimate URLs

Sectors Targeted: All

Motive: LokiBot malware delivery, data theft

Threat Actor(s)/Origin: Unknown

Platforms Affected: Windows

Report: [BleepingComputer](#)

Phishing Campaign Uses Political and Election Lures to Deliver Emotet

Synopsis: Emotet threat actors have dispersed several politically themed email campaigns days after the first 2020 US Presidential debate. These campaigns are designed to take advantage of the voters’ desire to have immediate media coverage of the election by promising to provide the recipient with useful information. These emails deliver a Word document attachment titled “Team Blue Take Action” embedded with malicious macros designed to download and install Emotet onto the victim’s computer.

Masquerades as: Political and Election Related Material

Sectors Targeted: All

Motive: Data theft, deliver additional malware

Threat Actor(s)/Origin: Unknown

Platforms Affected: Windows

Report: [Proofpoint](#)

Phishing mitigation recommendations: The NTIC Cyber Center recommends users remain vigilant for these and other phishing campaigns and be wary of unexpected emails, text messages, and social media messages. Additionally, refrain from clicking on links or opening attachments sent from unknown or untrusted sources and never enable content or macros on Microsoft Office documents before verifying their legitimacy. If you believe you have been infected with malware or have had your login credentials stolen as a result of a phishing campaign, notify your organization’s IT security team immediately. To learn how to identify phishing emails, please see the NTIC Cyber Center’s product titled [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

New and Notable Malware Campaigns**Cross-Platform Malware Affects Windows and Linux**

Synopsis: Security researchers have analyzed a newly documented cross-platform malware written in the Golang programming language named “InterPlanetary Storm” (IPStorm) that targets both Windows and Linux platforms. IPStorm turns a victim’s infected device into a botnet by abusing a legitimate peer-to-peer (p2p) network called InterPlanetary File System (IPFS), which provides the threat actor with the ability to execute arbitrary PowerShell commands on the victim’s device.

Sectors Targeted: All

Motive: To add new devices to a botnet

Threat Actor(s)/Origin: Unknown

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

Platforms Affected: Linux, Windows

Attack Vector: InterPlanetary File System

Mitigation Recommendations: The NTIC Cyber Center recommends administrators of enterprise servers apply the vendor-supplied patches to mitigate vulnerabilities as soon as possible, place network devices behind a firewall, disable unneeded SSH and Telnet connections, use lengthy, complex, and unique administrator credentials, and regularly monitor devices for unauthorized user accounts and access; To determine if your system has been compromised by IPStorm, please consult the directions provided in the Intezer report titled [A Storm Is Brewing: IPStorm Now Has Linux Malware](#).

Cryptojacking Malware Gang Targets Exposed Docker Daemon APIs

Synopsis: Palo Alto's research group is investigating a new strain of cryptojacking malware dubbed Black-T that targets exposed Docker daemon APIs. This specific malware installs three different variants of network scanners that are used to locate additional exposed Docker daemon APIs. This threat group also leverages a memory scraping tactic after successfully compromising the cloud system and exfiltrating stolen credentials.

Sectors Targeted: All

Motive: Credential Theft

Threat Actor(s)/Origin: TeamTnT

Platforms Affected: Linux

Attack Vector: Exposed Docker daemon

Associated CVEs: N/A

Mitigation Recommendations: Review [Docker's security guidance](#) and properly secure [Docker daemon sockets](#), secure all cloud administrator accounts with lengthy, complex and unique passwords, and enable multifactor authentication; proactively block IoCs contained in this report: [Palo Alto](#)

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data and organization at risk. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

New "Vaccine" Stops Ransomware from Deleting Shadow Volume Copies

An independent security researcher recently released a free ransomware "vaccine" called Raccine that monitors systems for the deletion of shadow volume copies via the execution of vssadmin.exe. Many ransomware variants launch vssadmin during the infection process to prevent victims from restoring data from shadow volume copies, a feature of Microsoft Windows that creates backup copies and snapshots of files. Raccine is designed to monitor the use of vssadmin and, if it detects that it is being used to delete shadow volume copies, it will automatically terminate the process. Although Raccine will not stop ransomware from encrypting files or spreading through a network, if configured properly, it could help victims recover their files without having to pay the ransom. For more information and instructions on how to install and use Raccine, please see BleepingComputer's article [here](#).

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER**Ransomware Operators Now Threaten Victims with DDoS Attacks**

Throughout 2020, several ransomware campaigns have added additional extortion tactics to coerce victims into paying ransom demands, including the threat of releasing sensitive data to the public and charging additional amounts for the deletion of stolen data. In a recent [attack](#), a SunCrypt ransomware operator targeted a victim who did not pay with a distributed denial-of-service (DDoS) attack that prevented legitimate network traffic from reaching the victim's website. The operator then threatened to continue the DDoS attack unless the victim agreed to pay the ransom. This incident highlights the increasing sophistication of profit-motivated ransomware operators as they employ a multitude of attacks to coerce victims to pay ransom demands.

New Jersey Hospital Pays Ransom to SunCrypt Attackers

A ransomware campaign known as SunCrypt [compromised](#) the University Hospital New Jersey (UHNJ) in Newark, New Jersey demanding a \$670,000 ransomware to prevent the publishing of 240 GB worth of stolen data. The SunCrypt threat actors initially published a sample of the hospital's data containing an archive of 48,000 documents on a leak site to pressure UHNJ to pay the ransom. A UHNJ representative corresponded with the threat actors via their dark web payment portal to negotiate the payment and prevent any further publishing of sensitive patient data. The threat actors gained access to UHNJ's network via a phishing email that tricked an employee into providing their network credentials. These credentials were then leveraged to gain access to UHNJ's Citrix server and the network.

Data Leaks and Breaches

Mobile-based food delivery service Chowbus [disclosed](#) a breach affecting restaurant vendors and its customers' data. The threat actors emailed links to the compromised data to all customers in two batches. The first batch contained data for 4,300 associated restaurants that included restaurant names, phone numbers, commission rates, and addresses. The second batch contained data of 803,350 users that included associated email addresses, names, phone numbers, and physical addresses. Chowbus is currently investigating the breach and has stated that the exposed data did not include financial information or passwords. ***The NTIC Cyber Center recommends that affected Chowbus users remain vigilant for phishing campaigns that result from this breach, change any passwords associated with their account, and continuously monitor accounts for any unauthorized or suspicious activity.***

Securing Our Communities

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



Mortgage wire fraud, also known as a mortgage closing scam, is a type of social engineering scheme in which perpetrators steal money or elicit personally identifiable information (PII) from victims through fraudulent real estate correspondence for financial gain or identity theft. Perpetrators take advantage of the numerous steps taken and parties involved in the real estate acquisition process. They target victims using email, voice messaging services, and websites. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

[\\$15 Million Business Email Scam Campaign in the US Exposed](#)

Analytic Comment: In ongoing global business email compromise (BEC) campaigns, cyber threat actors have stolen at least \$15 million from approximately 150 victims. Leveraging social engineering techniques via Microsoft Office 365 email services, cyber threat actors are masquerading as "senior parties" in transaction-related email chains and provide fraudulent wiring instructions that deviate from the original protocols. Researchers analyzed these BEC scams and believe that "each cluster was a coordinated attack on its own." This underscores the need for organizations to maintain awareness of the increasing prevalence and dangers of BEC scams. For more information on BEC scams, please read our piece titled [Securing Our Committees: Business Email Compromise](#).

[How Hackers Took Over Facebook Accounts to Steal \\$4 Million, Promote Scams](#)

Analytic Comment: A Chinese cybercrime network is responsible for a social media scam that stole more than \$4 million from Facebook users over several years. Using malware dubbed [SilentFade](#), the attackers stole social media accounts from legitimate users to commit ad fraud and steal funds from payment methods linked to the victims' accounts. Since the malware exploited vulnerabilities in users' browsers and not the platform itself, Facebook was initially unable to detect or mitigate the campaign. This highlights the need for social media users to maintain awareness of these types of threats, scrutinize links and ads posted on social media, and to enable multifactor authentication on any account that offers it.

Patches and Updates

[Google Releases Security Updates for Chrome](#)

ICS-CERT Advisories

[Wibu-Systems CodeMeter \(Update B\)](#)



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM

Cyber Center

Weekly Cyber Threat Bulletin

15 October 2020
Product No. 2020-10-020
NTIC SIN No. 2.5 | HSEC SIN No. 1

National Capital Region Cyber Threat Spotlight



BazarLoader Malware Used to Facilitate Ryuk Ransomware Attacks

The threat actors behind the Trickbot ransomware are progressively [targeting](#) high-value enterprise networks with BazarLoader/BazarBackdoor, a stealthy Trojan that can act as a downloader or dropper for other malware, such as Ryuk ransomware. Since Trickbot is currently much easier to detect, its operators have been using BazarLoader to bypass security controls. BazarLoader is described as a covert malware that obfuscates itself on the host system and uses process hollowing to inject its backdoor portion into legitimate Windows processes. Afterwards, it sets up a Cobalt Strike beacon that grants threat actors remote access who then deploy post-exploitation tools and Ryuk ransomware to infect networks. It is believed that BazarLoader is used to target specific victims rather than large campaigns. *The NTIC Cyber Center recommends users remain vigilant for BazarLoader phishing campaigns, avoid opening and unexpected emails, and refrain from clicking on links or opening attachments sent from unknown or untrusted source and never enable content or macros on Microsoft Office documents before verifying their legitimacy. If you believe you have been infected with BazarLoader notify your organization's IT security team immediately.*

Current and Emerging Cyber Threats

Common Malicious Email Attachments That Target Windows Systems

Malicious emails often include [attachments](#) or links to malicious Word and Excel files containing macros designed to deploy malware such as BazarLoader, Dridex, Emotet, and QakBot on targeted computers. Threat actors trick users into viewing these malware-laden documents by disguising them as invoices, invites, payment information, shipping information, eFaxes, voicemails, and others. In order to view contents "correctly," threat actors urge users to click the "Enable Content" or "Enable Editing" prompt so the malicious macros compromise the system. Additionally, threat actors email password-protected ZIP files to bypass email security gateways and may use files with the following extensions to execute commands: .vbs, .js, .exe, .ps1, .jar, .bat, .com, or .scr. While Microsoft hides file extensions by default,

TLP: WHITE

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

users may change these settings to view them. *The NTIC Cyber Center recommends users remain vigilant for malicious email campaigns, avoid opening and unexpected emails, and refrain from clicking on links or opening attachments sent from unknown or untrusted sources, enable settings to view extensions and never enable content or macros on Microsoft Office documents before verifying their legitimacy. If you believe you have been infected with malware or have had your login credentials stolen as a result of a phishing campaign, notify your organization's IT security team immediately.*

Private Information from Fairfax County Public Schools Breach Posted to Dark Web

The Fairfax County Public Schools superintendent has [confirmed](#) that data stolen from a September 11, 2020 Maze ransomware attack had recently been published on the dark web. The district sent out emails informing compromised staff, students, and families of the published data and that Virginia State Police and Federal Bureau of Investigation (FBI) are conducting criminal investigations. This incident highlights the cyber threats that the education sector faces as a result of virtual learning environments and limited IT resources. According to an analyst with Emsisoft, the Maze threat actors have removed Fairfax County Public Schools from their extortion blog.



IRS COVID Relief Phishing Campaign

Synopsis: Armorblox researchers report observing a malicious and fraudulent Internal Revenue Service (IRS) phishing campaign that promises its recipients COVID-19 related financial benefits if they choose to enroll in a program. Embedded in the email is a malicious link that directs to a SharePoint form designed to obtain and capture the victim's name, user credentials, Social Security number, driver's license number, and tax information.

Masquerades as: IRS COVID Relief Funds

Sectors Targeted: All

Motive: Credential Theft

Threat Actor(s)/Origin: Unknown

Platforms Affected: All

Report: [Armorblox](#)

Phishing mitigation recommendations: The NTIC Cyber Center recommends users remain vigilant for these and other phishing campaigns and be wary of unexpected emails, text messages, and social media messages. Additionally, refrain from clicking on links or opening attachments sent from unknown or untrusted sources and never enable content or macros on Microsoft Office documents before verifying their legitimacy. If you believe you have been infected with malware or have had your login credentials stolen as a result of a phishing campaign, notify your organization's IT security team immediately. To learn how to identify phishing emails, please see the NTIC Cyber Center's product titled [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

New and Notable Malware Campaigns

New Remote Access Trojan Malware Developed Using Golang Programming Language

Synopsis: Bitdefender researchers have discovered a new remote access Trojan (RAT) malware written in the Golang programming language targeting a Oracle WebLogic Servers vulnerability that has a Common Vulnerability Scoring System (CVSS) score of 9.8.

Sectors Targeted: All

Motive: RAT Infection

Threat Actor(s)/Origin: Unknown

Platforms Affected: Oracle WebLogic Servers

Attack Vector: Oracle WebLogic Servers

Associated CVEs: [CVE-2019-2725](#)

Mitigation Recommendations: The NTIC Cyber Center recommends administrators of Oracle WebLogic Services apply the latest security patches as soon as possible and block IoCs identified in this [report](#).

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data and organization at risk. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

Clop Ransomware Compromises Software AG

The threat actors behind the Clop ransomware variant [compromised](#) Software AG, a global enterprise software provider, demanding a \$23 million ransom to prevent the publishing of stolen data consisting of employee information and company documents. The ransomware was first noticed on Software AG's IT infrastructure early October. The evidence suggests that data was downloaded from Software AG's servers and employee notebooks. Software AG stated that the ransomware only affected its internal network and its customer cloud services were unaffected. Software AG is currently restoring its systems and data in order to resume normal operations.

Ransomware Threat Actors Turn to Third Party Network Access Sellers for Exploits

Analysts with Accenture's Cyber Threat Intelligence (CTI) team [reported](#) that ransomware threat actors are buying network access points and already compromised exploits from network access sellers to infiltrate and target system more efficiently, instead of relying on in-house capabilities. The researchers suggest a connection between ransomware threat groups and network access sellers based on shared dark web platforms, the types of industries targeted, and the access used to victimize organizations. These dark web platforms are known to support ransomware threat groups like Maze, NetWalker, Sodinokibi,

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM CYBER CENTER

Lockbit, and Avaddon, and, as of September this year, Accenture has tracked over 25 persistent network access sellers entering these dark web markets on a "weekly basis."

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



Fleeceware apps are mobile device applications that charge users high subscription fees after the app's free trial period ends. Often advertised as utility or gaming apps such as QR code readers, calculators, fortune telling apps, instant messengers, screen recorders, and photo or video editors, fleeceware apps often appear to have high installation counts and countless positive reviews on app marketplaces. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

[Most Counties' Election Sites Still Lack .gov and HTTPS, McAfee Says](#)

Analytic Comment: According to cybersecurity firm McAfee, the majority of US county election administrator-operated websites are missing major security features that would help users verify authentic websites that belong to their local officials. A review of websites under the county boards of elections in all states reveal that 45 percent did not use the HTTPS protocol that impedes users from being redirected to third-party or malicious sites and only about 20 percent have moved their websites to the official federal .GOV top-level domain. This is concerning as .COM, .NET, .ORG, and .US domain names can be acquired without the same level of restrictions compared to that of .GOV domains. According to McAfee, it is possible for threat actors to masquerade as legitimate election websites to spread disinformation. This underscores the importance of updating security features to highest standards to mitigate risks.

Patches and Updates

[Adobe Releases Security Updates for Flash Player](#)
[Apache Releases Security Updates for Apache Tomcat](#)
[Cisco Releases Security Updates](#)
[Microsoft Releases October 2020 Security Updates](#)
[QNAP Releases Security Updates for QNAP Helpdesk](#)
[SAP Releases October 2020 Security Updates](#)

ICS-CERT Advisories

[Fieldcomm Group HART-IP and hipserver](#)
[ICSA-17-332-01 Siemens SCALANCE W1750D, M800, S615, and RUGGEDCOM RM1224 \(Update C\)](#)
[LCDS LAquis SCADA](#)
[MOXA NPort IAW5000A-I/O Series](#)
[Siemens Desigo Insight](#)
[Siemens Industrial Products \(Update A\)](#)
[Siemens Industrial Products \(Update J\)](#)
[Siemens SIMATIC S7-300 and S7-400 CPUs \(Update A\)](#)
[Siemens SIPORT MP](#)



NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM

Cyber Center

Weekly Cyber Threat Bulletin

22 October 2020

Product No. 2020-10-032

NTIC SIN No. 2.5 | HSEC SIN No. 1

National Capital Region Cyber Threat Spotlight



NSA: Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities

On October 20, 2020, the National Security Agency (NSA) released a Cybersecurity Advisory on Chinese state-sponsored malicious activity. This advisory contains a list of CVEs that Chinese state-sponsored cyber actors are actively using against victim organizations within the US. Most of the vulnerabilities listed can be exploited to gain initial access to victim networks using products that are directly accessible from the internet and act as gateways to internal networks and should be prioritized for patching. ***The NTIC Cyber Center recommends all network administrators review the NSA's [Cybersecurity Advisory](#) and follow the recommended mitigation guidance provided.***

Current and Emerging Cyber Threats

Nano Adblocker and Nano Defender Adblocking Extensions Compromised

Researchers [report](#) that Nano Adblocker and Nano Defender adblocking browser extensions have been compromised, stealing data from users and gaining unauthorized access to users' online accounts. After the developer of the Nano Adblocker and Defender extensions sold the rights to new developers, users began reporting suspicious activity affecting social media accounts they had accessed using the same browser containing the extension. Researchers who tested the extensions noted that they were quietly uploading user data to a remote server. ***The NTIC Cyber Center recommends all Nano Adblocker and Nano Defender users remove these browser extensions immediately and change login credentials of any online account accessed via the affected browser. We also recommend monitoring online accounts accessed with affected browsers for suspicious activity.***

Hackers Selling Access to More Than 50,000 Compromised Home Security Cameras

A hacking group is selling access to more than 50,000 [compromised](#) home security cameras containing private footage of unsuspecting individuals, including children. This unnamed hacking group consists of more than 1000 members worldwide and has reportedly shared over 3TB worth of footage to their paid

TLP: WHITE

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

subscribers. Some of these clips have been posted to adult websites and free samples of these clips are reportedly available on other websites as well. It is likely that these clips originated from vulnerable and improperly secured IP security cameras. ***The NTIC Cyber Center encourages users and administrators of home security camera systems to immediately change any default passwords upon installation. We recommend using lengthy, complex, and unique passwords and enabling two-factor authentication (2FA) when available to provide an added layer of security for all IoT devices.***

Iranian APT Group Silent Librarian Targets Academic Institutions

Researchers at Malwarebytes recently observed Iranian Advanced Persistent Threat (APT) group Silent Librarian (also known as TA407 and Cobalt Dickens) actively targeting research materials of several universities worldwide. This group targets victims with spear phishing attacks that contain links to phishing pages mimicking university login pages. The domains associated with these pages share the same naming convention as the real university website but uses a different top level domain (TLD). For instance, instead of the domain name ending in the common .edu TLD, the threat group uses a TLD such as .me, .tk, or .cf. Researchers suggest that this is a rapidly growing campaign intent on targeting academic institutions throughout the 2020-2021 year. ***The NTIC Cyber Center recommends users remain vigilant for phishing campaigns and network administrators proactively block the indicators of compromise (IoCs) contained in Malwarebytes Labs' [report](#).***



Massive Phishing Campaign Uses Redirector Domains to Target Microsoft Office 365 Credentials and Others

Synopsis: Email security company GreatHorn discovered a massive phishing campaign that uses redirector domains or subsidiary domains of legitimate companies to bypass corporate security filters and target enterprise users' email and application credentials. The threat actors behind this campaign also use these phishing pages to deliver malware to victims.

Masquerades as: Password expiration notifications for Microsoft Office 365 accounts, Microsoft Teams, and Zoom

Sectors Targeted: All

Motive: Credential Theft

Threat Actor(s)/Origin: Unknown

Platforms Affected: Windows

Report: [Greathorn](#)

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER**Phishing Campaign Masquerades as the US Election Assistance Commission (EAC)**

Synopsis: Researchers have discovered a phishing campaign masquerading as the US Election Assistance Commission (EAC) distributing fraudulent voter registration forms to steal personally identifiable information (PII) such as Social Security numbers, tax identification numbers, and driver's license numbers.

Masquerades as: US Election Assistance Commission (EAC) correspondence

Sectors Targeted: All

Motive: PII theft

Threat Actor(s)/Origin: Unknown

Platforms Affected: All

Report: [Proofpoint](#)

Phishing mitigation recommendations: The NTIC Cyber Center recommends users remain vigilant for these and other phishing campaigns and be wary of unexpected emails, text messages, and social media messages. Additionally, refrain from clicking on links or opening attachments sent from unknown or untrusted sources and never enable content or macros on Microsoft Office documents before verifying their legitimacy. If you believe you have been infected with malware or have had your login credentials stolen as a result of a phishing campaign, notify your organization's IT security team immediately. To learn how to identify phishing emails, please see the NTIC Cyber Center's product titled [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

New and Notable Malware Campaigns**Mirai Variants Target New IoT Vulnerabilities**

Synopsis: Palo Alto Unit 42 researchers discovered four Mirai malware variants targeting two newly-discovered IoT vulnerabilities.

Sectors Targeted: All

Motive: DDoS attacks

Threat Actor(s)/Origin: Unknown

Platforms Affected: IoT devices

Attack Vector: IoT vulnerability exploitation

Associated CVEs: Please review all available listed CVE's [here](#).

Mitigation Recommendations: The NTIC Cyber Center recommends network administrators keep all IoT device firmware updated, place IoT devices behind a firewall, and proactively block the IoCs provided in Palo Alto's report titled [Two New IoT Vulnerabilities Identified with Mirai Payloads](#).

Ransomware Roundup

Welcome to Ransomware Roundup, a feature in the NTIC Cyber Center's Weekly Cyber Threat Bulletin where we shine a spotlight on new and emerging ransomware campaigns that put your data and organization at risk. To help improve your organization's cybersecurity posture, we encourage you to download and review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER**Iranian Nation-State Group Linked to Thanos Ransomware Attacks**

Security researchers at ClearSky and Profero have [linked](#) two ransomware campaigns targeting unpatched Microsoft Exchange servers to a known Iranian APT group dubbed “MuddyWater.” The first attack observed was a phishing campaign that contained either a malicious Microsoft Excel spreadsheet or a PDF document that, if opened, would download and install Thanos ransomware. The second attack exploited unpatched Microsoft Exchange servers by targeting the [CVE-2020-0688](#) vulnerability, allowing the threat actor to install a web shell on the compromised server to deploy Thanos ransomware.

Four Prominent Ransomware Families Emerge

Ransomware is a popular attack method among cyber criminals and some of the more [lucrative](#) campaigns include double extortion methods such as threatening to leak stolen data if victims fail to remit ransom payments to restore their encrypted data. According to cybersecurity researchers at Digital Shadows, 80 percent of ransomware attacks combined with data dumps were attributed to four ransomware families in the past three months – Maze, Sodinokibi, Conti, and Netwalker. Conti and NetWalker have risen to be the top two ransomware variants raking in more than \$100,000 worth of Bitcoin. The criminal competition within the ransomware landscape has caused a saturation within the ransomware market as developers strive to create the most popular variant. While ransomware continues to be a growing continued threat, proactive steps taken by organizations can help reduce the risk of a successful attack.

FIN11 Group Switches Tactics to Leverage Ransomware

Cyber threat group FIN11, known to use phishing and malware campaigns to [target](#) victims worldwide primarily in the finance, retail, and restaurant sectors, have pivoted into deploying ransomware indiscriminately throughout a wide variety of sectors. This is due to ransomware's efficiency, becoming one of the top money-making schemes for cyber threat actors. Once compromised, multiple backdoors are created, allowing attackers to move laterally across networks and pilfer credentials. FIN11 initiates these ransomware attacks with several thousand phishing emails simultaneously sent to multiple organizations at any single time. These phishing emails lure victims into downloading malicious Microsoft Office attachments and enabling macros that deploy the malicious payload. Researchers state that FIN11 is purely financially motivated and is still known to send out custom phishing campaigns on a target by target basis.

Vulnerabilities**SonicWall VPNs Vulnerable to Remote Code Execution**

A critical buffer overflow [vulnerability](#) [CVE-2020-5135](#) has been discovered in select SonicWall VPNs allowing remote unauthenticated threat actors to execute arbitrary code on vulnerable devices. Researchers state that over 800,000 VPN devices running vulnerable SonicOS software versions are impacted. While researchers have not observed any indications to date that CVE-2020-5135 has been exploited by attackers in the wild, an increase of remote workers on corporate VPNs make this and other similar vulnerabilities a concern. SonicWall has since released patches to remediate the flaw. ***The NTIC Cyber Center recommends all administrators of affected SonicWall VPNs update to the latest version as soon as possible.***

Data Leaks and Breaches

Barnes & Noble

Major US book retailer Barnes & Noble disclosed a [data breach](#) in which customer data was exposed. The breach is attributed to a cyber attack in which threat actors were able to gain access to corporate systems and disrupt services. Information compromised in this breach includes customers' email addresses, billing addresses, shipping addresses, and purchase history. Barnes & Noble has since restored systems back to operational order and has stated that the exposed data did not include payment details or other personal information. ***The NTIC Cyber Center recommends that affected Barnes & Noble users remain vigilant for phishing campaigns that result from this breach, change any passwords associated with their account, and continuously monitor accounts for any unauthorized or suspicious activity.***

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to help reduce their risk of becoming a victim of financial fraud and identity theft.



Car warranty scams are profit-motivated social engineering schemes designed to trick unsuspecting car owners into purchasing an extended warranty or service contract for their vehicles. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

Cyber in the News

[Closing the Expertise Gaps in State and Local Security](#)

Analytic Comment: State and local governments are starting to leverage managed and professional IT services to handle dynamic IT issues, especially when it comes to security. This helps with common struggles such as issues associated with legacy systems, service outages, remote workers, staff shortages, budget cuts, and cyber attacks. While the introduction of cloud services, high-speed mobile and SD-WAN networks, APIs, containers, and AI have allowed organizations to produce unprecedented results, the operating environment has become staggeringly complex. This has caused a vacuum in talent as it has been harder for IT departments to find and retain skilled workers. With an abundance of technological solutions on the market, more organizations may want to consider leveraging managed and professional IT services to handle complex IT problems and security solutions to supplement their in-house staff.

NATIONAL CAPITAL REGION THREAT INTELLIGENCE CONSORTIUM
CYBER CENTER

Patches and Updates

[Adobe Releases Security Updates for Magento](#)

[Adobe Releases Security Updates for Multiple Products](#)

[Google Releases Security Updates for Chrome](#)

[Microsoft Releases Security Updates to Address Remote Code Execution Vulnerabilities](#)

[Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird](#)

[VMware Releases Security Updates for Multiple Products](#)

ICS-CERT Advisories

[Advantech R-SeeNet](#)

[Advantech WebAccess/SCADA](#)

[Capsule Technologies SmartLinx Neuron 2 \(Update A\)](#)

[Hitachi ABB Power Grids XMC20 Multiservice-Multiplexer](#)

[Rockwell Automation 1794-AENT Flex I/O Series B](#)

[WECON LeviStudioU \(Update A\)](#)

[Wibu-Systems CodeMeter \(Update C\)](#)



Cyber Center

WEEKLY CYBER THREAT DIGEST

20 November 2020

Product No. 2020 11 022

NTIC SIN No. 2.5 | HSEC SIN No. 1

Emerging Cyber Threats & Trends

Healthcare Breaches Predicted to Triple in 2021

Data breaches in the healthcare industry are likely to [triple in volume](#) in the coming year, according to a new report by Black Book Market Research. Nearly 75% of health systems, hospitals, and physician organizations surveyed reported that their infrastructures are unprepared to respond to attacks. Almost all (96%) felt that data attackers are outpacing their medical enterprises, placing providers at a disadvantage. A further survey of 291 healthcare industry human resources executives found that the talent shortage of cybersecurity professionals far exceeds the cybersecurity demands by health systems. Researchers found that cybersecurity roles in healthcare take, on average, 70% longer to fill than other IT jobs.

Ransomware Attacks Against Education Sector up 388% in Q3 2020

The number of successful ransomware attacks on the education sector [increased by 388%](#) in the third quarter of 2020. The education sector reported 31 ransomware incidents in Q3 2020, compared with 8 incidents that occurred in the previous quarter. Nine of the 31 Q3 ransomware attacks involved data exfiltration, a common tactic among ransomware gangs over the past year.

Users Have Yet to Adopt Strong Passwords

After [analyzing nearly 300 million passwords](#) leaked during 2020 data breaches, password manager NordPass and its partners found that the most common passwords are incredibly easy to guess -- it could take less than a second or two for attackers to break into accounts using these credentials. Only 44% of passwords recorded were considered "unique." The password manager solutions provider's annual report on the state of password security found that the most popular options were "123456," "123456789," "picture1," "password," and "12345678." Most of these would take seconds to crack using either dictionary scripts -- which compile common phrases and numerical combinations to try -- or simple, human guesswork. As one of the entrants on the 200-strong list of most popular passwords, "whatever," aptly captures, there continues to be widespread reluctance to use strong, unique passwords.

Data Leaks and Breaches

The North Face Breach

The North Face [has reset its customers' passwords](#) after attackers launched a credential-stuffing attack against the popular outdoor outfitter's website, thenorthface.com. In addition to email addresses and passwords, cybercriminals may have accessed customer account information including billing and shipping addresses, loyalty point totals, email preferences, first and last names, birthdays, and telephone numbers.

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

This personal data is vulnerable to abuse by social-engineers for phishing attacks. Credential stuffing occurs when hackers take advantage of people who reuse their passwords across multiple online accounts. The attackers typically use stolen IDs and passwords obtained via a breach of one company or website, and then use them to gain unauthorized access to other accounts. The process is often automated; cybercriminals have successfully leveraged the technique to steal data from popular companies.

123RF Breach

Stock photo site 123RF [has suffered a data breach](#) after a hacker began selling a database containing 8.3 million user records on a hacker forum. The stolen data includes 123RF members' full names, email addresses, MD5 hashed passwords, company names, phone numbers, addresses, PayPal emails, and IP addresses. There is no financial information stored in the database.

The NTIC Cyber Center recommends affected consumers apply for free credit monitoring services if offered by the compromised company; monitor bank and credit card statements closely; immediately report any unauthorized activity to their financial institutions; ensure new passwords are lengthy, complex, and unique to each account; and enable multifactor authentication when available. Victims of this or other data breaches are encouraged to visit the Federal Trade Commission's online [identity theft resource page](#) and consider placing a fraud alert or security freeze on their credit file.

Phishing Campaigns

Microsoft Office 365 Phishing Campaign

An ongoing Office 365 phishing campaign attacking enterprise targets [uses several methods to evade detection](#) by automated analysis. One of these tactics is the use of redirector URLs that detect and avoid incoming connections from sandbox environments commonly used by security researchers seeking to gain more information about the attack. Once such a connection is detected, the redirector will switch from sending potential victims to a phishing landing page to redirecting the automated analysis attempts to legitimate sites. This allows the phishers to make sure that their phishing pages will only be visited by real users, thus drastically lowering the chance of their attacks being discovered and blocked, and increasing the odds of real people being lured to the phishing sites.

The NTIC Cyber Center recommends remaining vigilant for phishing or social engineering attempts conducted through URLs, websites, emails, texts, phone calls, voicemails, social media, or alternative messaging platforms. We encourage the use of lengthy, complex, and unique passwords for each account. We also urge users to enable multifactor authentication when available to avoid falling victim to account compromise. Additionally, avoid opening unexpected correspondence and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. Never provide sensitive and personal information in response to unsolicited correspondence. If you believe you have been targeted by a malicious campaign or had credentials or personal information compromised, notify your IT security team immediately. To learn more, please see the NTIC Cyber Center's product [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Malware Campaigns

Managed.com Ransomware Attack

Managed.com, one of the biggest providers of managed web hosting solutions, [has taken down](#) all its servers to deal with a ransomware attack. The ransomware impacted the company's public-facing web hosting systems, and attackers have encrypted data on some of Managed.com's customer sites. Managed.com said it immediately took these sites offline. Hours after the attack, the company announced it had also taken down its entire web hosting infrastructure. This included WordPress and DotNetNuke-managed hosting solutions, email servers, DNS servers, RDP access points, FTP servers, and databases. The company is working with law enforcement to identify the attackers and restore customer systems as soon as possible.

The NTIC Cyber Center recommends maintaining regular system backups; monitoring network traffic for suspicious activity; securing connection services; and keeping all devices, applications, antivirus platforms, and operating systems patched and up-to-date. We also recommend decommissioning any unsupported or end-of-life (EOL) systems and software. In addition, users should avoid using domain-wide, administrator-level service accounts, avoid clicking on unknown links in correspondence, and refrain from downloading content from untrusted sources. We encourage using lengthy, complex, and unique passwords for each account, and enabling multifactor authentication when available to avoid account compromise. To improve your organization's cybersecurity posture, we encourage you to review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on [our website](#).

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to reduce their risk of becoming a victim of financial fraud and identity theft.



Mortgage wire fraud, also known as a mortgage closing scam, is a type of social engineering scheme in which perpetrators steal money or elicit personally identifiable information (PII) from victims through fraudulent real estate correspondence for purposes of financial gain or identity theft. Perpetrators take advantage of the numerous steps and parties involved in the real estate acquisition process. They target victims using email, voice messaging services, and websites. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

NTIC Cyber Center

CYBER THREAT DIGEST: BLACK FRIDAY/CYBER MONDAY SPECIAL EDITION



25 November 2020

Product No. 2020-11-028

NTIC SIN No. 2.5 | HSEC SIN No. 1

Emerging Cyber Threats & Trends

Online Retail Faces Unprecedented Security Risks This Black Friday Retailers must prepare for a Black Friday like no other. A new threat intelligence report illustrates the varying cybersecurity attack risks facing the retail industry, and the impact the global pandemic has had on the volume of attacks and web traffic. "[The State of Security within E-commerce](#)" suggests levels of traffic throughout the holiday shopping season will reach an unprecedented peak as a flood of consumers turn to online channels to purchase goods. The report details several concerning cyber-attack trends, including: bad bots abusing websites, mobile apps, and APIs, web attacks, DDoS attacks, account takeover (ATO) attacks and client-side attacks.

Black Friday— an Opportunity for DDoS Attacks

Black Friday is prime time for distributed denial-of-service (DDoS) attacks, especially as retail goes online even more than usual in 2020. Forecasters predict e-commerce sales will soar to new heights this holiday season, increasing by as much as 35% year-over-year. This explosion in online shopping brings new challenges to retailers, including managing logistics and supply chains. It also means that increased cyber threats targeting the retail industry are all but inevitable. While retailers should take measures to secure e-commerce infrastructures all year long, this year's Black Friday DDoS attacks may be especially challenging if they accompany exceptionally high volumes of normal traffic.

Fraud Alert! Buy Online, Pick-Up In Store (BOPIS) Schemes

COVID-19 restrictions have resulted in BOPIS options becoming necessities for many companies that lack the logistical capabilities or capital to deliver their goods to their customers' doors. Fraudsters know that many businesses are new to BOPIS fulfillment and are actively exploiting the system. Be on the lookout for account takeover (ATO) attacks that specifically target merchants offering BOPIS. Scammers are using stolen payment and account info to place orders. The ruse is easily executed once the fraudster changes a legitimate shopper's account information to their own or when they place the order with the shopper's real information and then insert their own name as the pick-up person, allowing them to bypass a cursory inspection.

Securing Our Communities

Stay Cyber Safe: Online Shopping & Cyber Risks Will Soar This Week

COVID-19 safety measures will likely contribute to an increase in the traffic to online retail websites this holiday season; millions of Americans are preparing for the busiest shopping time of the year. ***The NTIC Cyber Center expects online orders and cybersecurity risks associated with e-shopping will surge to unprecedented levels beginning this Thanksgiving and lasting until the end of 2020.*** To ease the burden on customers and to provide a cleaner shopping environment, many merchants have extended the duration of sales and are strongly encouraging customers to shop online.

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

This means cyber criminals are also preparing for lucrative opportunities to steal passwords, financial details, and personal information from busy, unsuspecting shoppers. To help protect yourself and your information, follow these tips to stay cyber safe while shopping this holiday season:

- **Strong Passwords and Multifactor Authentication (MFA):** The sale of stolen username and password combinations in dark web marketplaces is big business for cyber criminals. Recent large-scale data breaches have made it easier than ever for hackers to get their hands on your login information. Use a lengthy, complex, and unique password for each account to protect your online accounts from unauthorized access. To generate secure passwords and easily manage your login credentials, consider using a reputable password manager. Also, always enable multifactor authentication (MFA) on any account that offers it for an additional layer of security.
- **Beware of phishing websites and apps designed to steal your credentials and payment information.** Cyber criminals commonly build webpages and apps that masquerade as popular Internet shopping and banking services. Some even use valid digital certificates to make the websites appear legitimate. It is critically important to double-check the URL to make sure that you are using the real site or app, not a fake one. In addition, always check that the address of the website you are visiting starts with HTTPS (the "S" stands for "Secure"),
- **Look out for indications that a website may be compromised with a payment card skimmer.** Threat actors inject malicious code into e-commerce websites to steal payment card information from online shoppers. Always monitor your bank account statements closely for unauthorized charges and suspicious activity. Signs that a legitimate site may be compromised include:
 - Being asked twice to enter payment or login information
 - Being prompted to enter payment card details before being forwarded to a secure payment service provider
- **Use credit cards rather than debit cards.** If your payment card numbers are stolen or compromised, using credit cards can limit your liability for fraudulent charges. Debit cards often do not afford these same protections.
- **Never click on links or open attachments from unexpected or unknown sources.** Scammers distribute emails disguised as legitimate communications such as package tracking notifications, e-cards, charity donation requests, or purchase confirmations. Just one click can result in the compromise of your computer, information, and identity.
- **Protect delivered purchases from theft.** Thieves surveil and steal delivered goods from doorsteps. This year, they know more people are purchasing online more than ever. Track your package throughout its journey and be available to collect it when it arrives. Leverage friendly neighbors and security camera systems to keep guard. Requiring a signature on delivery will help mitigate theft risk as well.
- **If it sounds too good to be true, it probably is.** Be wary of anything that is advertised at extremely low prices. Scammers use these tactics to trick shoppers into visiting malicious or fraudulent websites. Even legitimate retailers may use the lure of deeply discounted products to trick shoppers into signing up for unwanted recurring subscription charges or additional items. This tactic is called "dark pattern manipulation;" it is important for online shoppers to recognize the signs before making any online purchase. Read the NTIC Cyber Center's blog post titled [Securing Our Communities: Dark Patterns](#) to learn more.

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Phishing Campaigns

Threat Actors Abuse a Wide Range of Google Services

A spike in recent [phishing](#) and business email compromise (BEC) attacks can be traced back to criminals who are learning how to exploit Google Services, according to research from Armorblox. Social distancing has driven entire businesses into the Google ecosystem as they seek a reliable, simple way to digitize the traditional office. Armorblox published a report detailing how ubiquitous services like Google Forms, Google Docs, and others are being used by malicious actors to give their spoofing attempts a false veneer of legitimacy, both to security filters and victims.

The NTIC Cyber Center recommends remaining vigilant for phishing or social engineering attempts conducted through URLs, websites, emails, texts, phone calls, voicemails, social media or alternative messaging platforms and encourages the use of lengthy, complex, and unique passwords for each account. We urge users to enable multifactor authentication when available to avoid falling victim to account compromise. Additionally, avoid opening unexpected correspondence and refrain from clicking on links, opening attachments, enabling macros in documents from unknown or untrusted sources. Never provide sensitive and personal information in response to unsolicited correspondence. If you believe you have been targeted by a malicious campaign or had credentials or personal information compromised, notify the relevant IT security teams immediately. Please see the NTIC Cyber Center's product [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

Malware Campaigns

Cyber Gang Hijacks WordPress Sites

A new cybercrime gang has been observed [taking](#) over vulnerable WordPress sites to install hidden e-commerce stores that hijack the original site's search engine ranking and reputation, and promote online scams. The attackers leveraged brute-force attacks to gain access to the site's admin account; they overwrote the WordPress site's main index file and appended malicious code. Cashdollar said the malware's primary role was to act as a proxy and redirect incoming traffic to a remote command-and-control (C&C) server managed by the hackers.

The NTIC Cyber Center recommends maintaining regular system backups; monitoring network traffic for suspicious activity; securing connection services; and keeping all devices, applications, antivirus platforms, and operating systems patched and up-to-date. We also recommend decommissioning any unsupported or end-of-life (EOL) systems and software. In addition, users should avoid using domain-wide, administrator-level service accounts and avoid clicking on unknown links in correspondence and downloading content from untrusted sources. We encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication when available to avoid account compromise. To improve your organization's cybersecurity posture, we encourage you to review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.



Cyber Center

WEEKLY CYBER THREAT DIGEST

04 December 2020

Product No. 2020-12-004

NTIC SIN No. 2.5 | HSEC SIN No. 1

Emerging Cyber Threats & Trends

Docker Malware Attacks On the Rise

Cyber threat actors have increasingly targeted Docker and Kubernetes systems, as cloud-based technologies have [become](#) more popular. Most of these attacks followed a pattern where threat actors scanned for misconfigured systems that had admin interfaces exposed online, allowing them to take over servers and deploy cryptocurrency-mining malware. Over the past three years, these attacks have intensified, and new malware strains and threat actors targeting Docker and Kubernetes are now discovered on a regular basis. Even though these malware attacks are now commonplace, many web developers and infrastructure engineers are still misconfiguring Docker servers and leaving them exposed to attacks. Most commonly, Docker remote administration API endpoints are left exposed online without authentication.

Botnet Operators Pivot to Ransomware Distribution

Most botnet operators have [dropped](#) banking Trojans in favor of running crypto-locking malware attacks. Ransomware gangs have been increasingly adopting affiliate programs, in which the ransomware operators building attack code and infrastructure, and then affiliates plant the malicious code on systems. Every time a victim pays, the affiliate and the operator share the profits in this lucrative scheme. From late 2019 to early 2020, 14 of the biggest ransomware gangs collectively shook down victims for at least \$1 billion in ransom payments.

Phishing and Fraudulent Sites Increase 13.3%

New phishing and fraudulent sites were created at an alarmingly rapid [rate](#) in Q2 this year. Research uncovered 1.7 million new phishing and scam websites – a 13.3% increase from Q1 2020. Phishing and scam websites continued to increase in Q2, peaking in June 2020 with a total of 745,000 sites. On average, more than 18,000 fraudulent sites were created each day. The most active phishing scammers use free emails accounts from trusted providers; Gmail was the most popular with over 45% of email addresses. According to the data, nearly 44,000 new phishing and fraudulent websites impersonated the top 10 online brands from January to September 2020.

Data Leaks and Breaches

Belden Data Breach

American networking equipment vendor Belden announced earlier this week that it had been [hacked](#). Belden stated that hackers gained access to a limited number of its file servers during the security breach. The intrusion was detected after the company's IT personnel detected unusual activity on the compromised servers. A subsequent investigation revealed that the intruders had copied some current and former employees' data, and company information regarding some business partners. Belden is notifying the affected customers and employees.

US Fertility Network Compromised

Cyber criminals [conducted](#) a ransomware attack on US Fertility, one of the largest networks for fertility clinics in the country. The attack exposed patient data. Digital forensic specialists found that although the ransomware had been triggered on September 14, the attackers had first penetrated the network a month earlier, on August 12. During this time, the attackers had access to patient data. Sensitive information accessed includes names, addresses, dates of birth, and Social Security numbers.

The NTIC Cyber Center recommends affected consumers apply for free credit monitoring services if offered by the compromised company; monitor bank and credit card statements closely; immediately report any unauthorized activity to their financial institutions; ensure new passwords are lengthy, complex, and unique to each account; and enable multifactor authentication when available. Victims of this or other data breaches are encouraged to visit the Federal Trade Commission's online identity theft [resource](#) page and consider placing a fraud alert or security freeze on their credit file.

Phishing Campaigns

"Return to Office" Phishing Campaign

Scammers are [impersonating](#) internal company memos about when the company will return to the office to steal employee credentials. These phishing emails contain an HTML attachment with the recipient's name designed to trick the recipient into opening it. When clicking on the attachment, the scam redirects the user to a SharePoint document that contains instructions on the company's remote working policy. Underneath the "new" policy, there is a button that says, "PROCEED WITH ACKNOWLEDGEMENT HERE". Clicking on this link sends the user to the attack landing page that harvests the employee's email credentials.

The NTIC Cyber Center recommends remaining vigilant for phishing or social engineering attempts conducted through URLs, websites, emails, texts, phone calls, voicemails, social media or alternative messaging platforms and encourages the use of lengthy, complex, and unique passwords for each account. We urge users to enable multifactor authentication when available to avoid falling victim to account compromise. Additionally, avoid opening unexpected correspondence and refrain from clicking on links, opening attachments, enabling macros in documents from unknown or untrusted sources. Never provide sensitive and personal information in response to unsolicited correspondence. If you believe you have been targeted by a malicious campaign or had credentials or personal information compromised, notify the relevant IT security teams immediately. Please see the NTIC Cyber Center's product [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

Malware Campaigns

Baltimore County Public Schools Hit by Ransomware

Public schools in Baltimore County, Maryland, were closed last Wednesday after the district's IT systems were disrupted by a [ransomware](#) attack. Both in-person and online classes were cancelled. The type of ransomware used in the attack has still not been identified. Baltimore county officials described the attack as a "systemic interruption to network information systems," and said that their IT team is working to remedy the issue. School officials also advised students and teachers not to use their school-issued devices.

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

The NTIC Cyber Center recommends maintaining regular system backups; monitoring network traffic for suspicious activity; securing connection services; and keeping all devices, applications, antivirus platforms, and operating systems patched and up-to-date. We also recommend decommissioning any unsupported or end-of-life (EOL) systems and software. In addition, users should avoid using domain-wide, administrator-level service accounts and avoid clicking on unknown links in correspondence and downloading content from untrusted sources. We encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication when available to avoid account compromise. To improve your organization's cybersecurity posture, we encourage you to review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to reduce their risk of becoming a victim of financial fraud and identity theft.



Counterfeit goods are fraudulent products that are similar or nearly identical to their legitimate counterparts and are typically sold for financial gain. While the sale of counterfeit goods is not a new practice, advances in technology and the popularity of e-commerce platforms have led to an increase in the prevalence of counterfeit goods distribution. Click [here](#) to read more about this prevalent scam and learn how to protect yourself.

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.



Cyber Center

WEEKLY CYBER THREAT DIGEST

11 December 2020

Product No. 2020-12-012

NTIC SIN No. 2.5 | HSEC SIN No. 1

Emerging Cyber Threats & Trends

Economic Impact of Global Cybercrime Exceeds \$1 Trillion

A research study [reveals](#) that cybercrime costs the world economy more than \$1 trillion, which is more than one percent of the global GDP. That figure is nearly 100 percent greater than a 2018 study that put global losses to cybercrime around \$600 billion. The 2020 report also explored damage from cybercrime beyond financial losses: 92% of companies felt effects beyond monetary losses. Some of the most overlooked costs of cybercrime include damage to company performance and hidden costs such as system downtime, reduced efficiency, incidence response costs, and brand and reputation impacts.

Vulnerabilities in Open Source Software take Over 4 Years to Detect

A recent study [reveals](#) that it takes an average of over four years to spot vulnerabilities in open source software. Reliance on open source projects, components, and libraries is more common than ever. According to GitHub, "Many of the services and technology we all rely on, from banking to healthcare, also rely on open source software. The artifacts of open source code serve as critical infrastructure for much of the global economy, making the security of open source software mission critical to the world. Even though the majority of bugs in open source software are not malicious (83% of the CVE alerts issued by GitHub have been caused by mistakes and human error), threat actors still take advantage of them for malicious purposes.

Data Leaks and Breaches

Verizon Leak Affected Customers' Personal Information

Verizon is [fixing](#) a glitch that has been leaking customers' addresses, phone numbers, account numbers, and other personal information through a chat system designed to help prospective subscribers figure out if Verizon Fios services are available in their location. The leaked personal details appear when users click on a link to chat with a Verizon representative; the chat window opens to display transcripts of conversations that other customers (prospective and current) have had with Verizon. Those transcripts include full names, addresses, phone numbers, account numbers, among other details. It is not clear when the data began leaking; with some of the chats dating back to June, it's possible that the leak has been occurring for months.

Recruitment Agency Hit by Ransomware Attack

One of the world's largest recruitment agencies, Randstad, [has](#) become the latest victim of a serious ransomware attack. It appears as if the firm managed to escape any major operational impact, but did suffer a data breach after being hit by the Egregor ransomware variant. The firm took action globally to mitigate the incident while further protecting its systems, operations and data. As a result, only a limited number of servers were impacted. An investigation into exactly which data was accessed is ongoing and the company intends to notify the affected parties. As a major recruiter, Randstad likely maintains personal data from job-seekers. The firm stated that the relevant regulatory authorities and law enforcement agencies have been notified, and that third-party systems do not appear to have been impacted by the attack.

The NTIC Cyber Center recommends affected consumers apply for free credit monitoring services if offered by the compromised company; monitor bank and credit card statements closely; immediately report any unauthorized activity to their financial institutions; ensure new passwords are lengthy, complex, and unique to each account; and enable multifactor authentication when available. Victims of this or other data breaches are encouraged to visit the Federal Trade Commission's online identity theft [resource](#) page and consider placing a fraud alert or security freeze on their credit file.

Phishing Campaigns

200 Million Microsoft Office Users Targeted

A spear-phishing attack [spoofed](#) Microsoft.com to target 200 million Microsoft Office 365 users in a number of key vertical markets, including financial services, healthcare, manufacturing, telecom, insurance and utility providers. The attack contains a realistic email that attempts to persuade victims to use a relatively new Office 365 capability that allows them to reclaim emails that have been accidentally marked as spam or phishing. When a user clicks on the link, they are asked to type in their Office 365 login credentials on a fake log-in page controlled by the attackers to harvest and, most likely, to sell the credentials on the dark web. The campaign is particularly deceiving because it deploys an exact domain spoofing technique, wherein an email is sent from a fraudulent domain that is an exact match to the spoofed brand's domain.

Cyber Threat Actors Target COVID-19 Vaccine Cold Chain

IBM's cyber-security division [says](#) that hackers are targeting companies managing the cold storage and transportation of COVID-19 vaccines -- also known as the COVID-19 vaccine cold chain. According to IBM, the attackers specifically targeted executives at each company; usually these were individuals working in sales, procurement, IT, and finance positions in which they were likely to be involved in efforts to support a vaccine cold chain. The selected targets received emails using the spoofed identity of a business executive from Haier Biomedical, a Chinese company that is part of the UN's official Cold Chain Equipment Optimization Platform (CCEOP) program.

The NTIC Cyber Center recommends remaining vigilant for phishing or social engineering attempts conducted through URLs, websites, emails, texts, phone calls, voicemails, social media or alternative messaging platforms and encourages the use of lengthy, complex, and unique passwords for each account. We urge users to enable multifactor authentication when available to avoid falling victim to account compromise. Additionally, avoid opening unexpected correspondence and refrain from clicking on links, opening attachments, enabling macros in documents from unknown or untrusted sources. Never provide sensitive and personal information in response to unsolicited correspondence. If you believe you have been targeted by a malicious campaign or had credentials or personal information compromised, notify the relevant IT security teams immediately. Please see the NTIC Cyber Center's product [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

Malware Campaigns

Ransomware Compromises Greater Baltimore Medical Center Computer Systems

The Greater Baltimore Medical Center (GBMC) [confirmed](#) Sunday evening that they detected a ransomware incident that downed some of their systems earlier that day. The GBMC stated that the incident impacted their IT systems, but that they have "robust processes" in place to maintain "safe and effective patient care." There is no evidence that any patient information was misused and GBMC is working with experts and law enforcement on the investigation.

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Cyber Threat Actors Target K-12 Distance Learning Education

The FBI, CISA, and MS-ISAC [assess](#) malicious cyber actors are targeting kindergarten through twelfth grade (K-12) educational institutions. Incidents include ransomware attacks that lead to data theft and the disruption of distance learning services. The government expects these attacks to continue through 2021. Cyber issues are particularly challenging for K-12 schools that face resource limitations. The five most common ransomware variants identified in these incidents between January and September 2020 are Ryuk, Maze, Nefilim, AKO, and Sodinokibi/REvil.

The NTIC Cyber Center recommends maintaining regular system backups; monitoring network traffic for suspicious activity; securing connection services; and keeping all devices, applications, antivirus platforms, and operating systems patched and up-to-date. We also recommend decommissioning any unsupported or end-of-life (EOL) systems and software. In addition, users should avoid using domain-wide, administrator-level service accounts and avoid clicking on unknown links in correspondence and downloading content from untrusted sources. We encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication when available to avoid account compromise. To improve your organization's cybersecurity posture, we encourage you to review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to reduce their risk of becoming a victim of financial fraud and identity theft.



The Secret Sister Gift Exchange is a type of pyramid scheme primarily targeting female Facebook users, in which perpetrators use the guise of an innocent holiday gift exchange to steal personal information from participants. In these scams, Facebook users send direct messages or emails to others, inviting them to participate in the exchange. To join, new recruits must provide their name and address, send one gift valued at \$10 to another participant, and forward the invitation to other women. In exchange, they are promised a return of up to 36 gifts from other participants and future recruits. Read this NTIC Cyber Center [report](#) to learn about this prevalent scam and how to protect yourself.

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.



Cyber Center

WEEKLY CYBER THREAT DIGEST

24 December 2020

Product No. 2020-12-028

NTIC SIN No. 2.5 | HSEC SIN No. 1

Emerging Cyber Threats & Trends

Common Vulnerabilities and Exposures (CVE) Break Record for 4th Consecutive Year

Records [indicate](#) a record number of CVEs this year for the fourth year in a row. As of December 15, the number of vulnerabilities discovered and assigned a CVE number by the US-CERT Vulnerability Database topped the 2019 figure. Last year there were 17,306 CVEs published, including 4337 high-risk, 10,956 medium-risk and 2013 low-risk flaws. Latest figures show that 17,447 were recorded in 2020 in total, including 4168 high-risk, 10,710 medium-risk and 2569 low-risk bugs. Between 2005-16 numbers ranged from around 4000 to 8000 vulnerabilities each year, according to the official figures from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database. However, in 2017 the number skyrocketed to over 14,000, and every year since published volumes have hit a record high.

Data Leaks & Breaches

Ledger Cryptocurrency Wallet Breach

A threat actor has [leaked](#) stolen email and mailing addresses for Ledger cryptocurrency wallet users on a hacker forum. Ledger is a hardware cryptocurrency wallet that is used to store, manage, and sell cryptocurrency. The cryptocurrency funds are secured using a 24-word recovery phrase and an optional secret passphrase that only the owner knows; however in June 2020, Ledger suffered a data breach after a website vulnerability allowed threat actors to access customers' contact details. Recently, the criminal shared the personal information of 272,853 people who purchased a Ledger device. The release of this data on a hacker forum poses a significant risk because it provides data that can be used by other threat actors in future phishing attacks against Ledger owners.

The NTIC Cyber Center recommends affected consumers apply for free credit monitoring services if offered by the compromised company; monitor bank and credit card statements closely; immediately report any unauthorized activity to their financial institutions; ensure new passwords are lengthy, complex, and unique to each account; and enable multifactor authentication when available. Victims of this or other data breaches are encouraged to visit the Federal Trade Commission's online identity theft [resource](#) page and consider placing a fraud alert or security freeze on their credit file.

Phishing Campaigns

US Federal Agencies Warn of COVID-19 Vaccine Fraud

US government agencies have [warned](#) about scammers exploiting the public's interest in the COVID-19 vaccine to harvest personal information and steal money through multiple ongoing and emerging fraud schemes. The FBI highlighted Potential indicators of such fraudulent activity including offers for early access to vaccines by advance payment, requests to pay out to receive a vaccine or to get added to a waiting list, and offers to ship vaccine doses in exchange for money transfers. The FBI advises you search for vaccine distribution information on your state health department's website to ensure not falling for scammers' fraud attempts.

The NTIC Cyber Center recommends remaining vigilant for phishing or social engineering attempts conducted through URLs, websites, emails, texts, phone calls, voicemails, social media or alternative messaging platforms and encourages the use of lengthy, complex, and unique passwords for each account. We urge users to enable multifactor authentication when available to avoid falling victim to account compromise. Additionally, avoid opening unexpected correspondence and refrain from clicking on links, opening attachments, enabling macros in documents from unknown or untrusted sources. Never provide sensitive and personal information in response to unsolicited correspondence. If you believe you have been targeted by a malicious campaign or had credentials or personal information compromised, notify the relevant IT security teams immediately. Please see the NTIC Cyber Center's product [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

Malware Campaigns & Vulnerabilities

Over Three Million Users Installed Malicious Browser Extensions

More than three million internet users are believed to have [installed](#) malicious Chrome and Edge extensions. The 28 extensions contained code that could perform several malicious operations including redirecting users to ads, redirecting users to phishing sites, collecting personal data, collecting browsing history, and downloading new malware onto users' devices. Researchers believe the primary objective of this malicious code is to hijack user traffic for monetary gain.

The NTIC Cyber Center recommends maintaining regular system backups; monitoring network traffic for suspicious activity; securing connection services; and keeping all devices, applications, antivirus platforms, and operating systems patched and up-to-date. We also recommend decommissioning any unsupported or end-of-life (EOL) systems and software. In addition, users should avoid using domain-wide, administrator-level service accounts and avoid clicking on unknown links in correspondence and downloading content from untrusted sources. We encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication when available to avoid account compromise. To improve your organization's cybersecurity posture, we encourage you to review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to reduce their risk of becoming a victim of financial fraud and identity theft.



Staying Safe This Holiday Season, as the holiday season rapidly approaches, millions of Americans are preparing for the busiest shopping time of the year. Unfortunately, cyber criminals are also preparing for the holidays along with the lucrative opportunities they bring to steal passwords, financial details, and personal information from busy, unsuspecting shoppers. Read [this](#) NTIC Cyber Center report to learn about this prevalent scam and how to protect yourself.

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

WEEKLY CYBER THREAT DIGEST

31 December 2020

Product No. 2020-12-035
NTIC SIN No. 2.5 | HSEC SIN No. 1

Emerging Cyber Threats & Trends

Smart Cars Can Be Hacked Like Other Connected Devices

Connected cars are complex systems [composed](#) of numerous units that exchange large amounts of data, and threat actors can manipulate those systems in order to gain control of smart vehicles. Security experts speculate that in some cases, car makers have failed to implement adequate protections from cyberattacks. Threat actors could hack a vehicle to steal sensitive data managed by its components for sabotage purposes, or simply to steal the car. Connected cars can share information with other vehicles in C2C (car-to-car) or C2I (car-to-infrastructure) connections in real-time. In essence, they are becoming sophisticated nodes of the global network that manages massive amounts of information.

Data Leaks and Breaches

User Data of 21 Buttons Social Network Exposed

The fashion social network, 21 Buttons, has [suffered](#) a data breach with the records of its users found exposed online. The data was found on an unsecured Amazon Web Services Inc. S3 cloud storage bucket. It included 50 million pieces of data, including social media posts and profiles, invoices, full names, addresses, postal codes, bank details, nation ID numbers, PayPal email addresses, and in some cases the value of sales commission earned through the app.

Card Skimmer Found on Multiple E-Commerce Platforms

A recently [discovered](#) multi-platform credit card skimmer can harvest payment information on compromised stores powered by Shopify, BigCommerce, Zencart, and Woocommerce. While card skimmers are usually designed to target a single type of e-commerce platform, this new type of web skimming malware can take over the checkout process on shops using multiple online store management systems by injecting a malicious checkout page. It does this by displaying a fake payment page before the customers land on the real checkout form and using a keylogger to intercept payment and personal information. The skimmer will also throw an error after the customers hit the "Proceed" button to submit their credit card information to evade detection and not raise any alarm flags, redirecting the customer back to the legitimate checkout process and payment form.

The NTIC Cyber Center recommends affected consumers apply for free credit monitoring services if offered by the compromised company; monitor bank and credit card statements closely; immediately report any unauthorized activity to their financial institutions; ensure new passwords are lengthy, complex, and unique to each account; and enable multifactor authentication when available. Victims of this or other data breaches are encouraged to visit the Federal Trade Commission's online [identity theft resource page](#) and consider placing a fraud alert or security freeze on their credit file.

Phishing Campaigns

Chase Bank Phishing Scam Masquerades as Fraud Notification

A large-scale phishing scam is [underway](#) that pretends to be a security notice from Chase Bank stating that fraudulent activity has been detected and has caused the recipient's account to be blocked. These phishing emails state that the recipient's Chase account was blocked after suspicious activity was detected. To "unlock" the account, the recipients are prompted to click on the "Restore Now" button

in the email. When the “Restore Now” button is clicked, the recipient will be brought to a page asking them to log in to their Chase account. If they enter their login information, it will be sent to the attackers, who will then have access to the account. The phishing page will further prompt the user to enter additional information about themselves to verify that they are the account owner. This additional information includes the recipient’s first and last name, date of birth, Social Security Number, address, and phone number.

The NTIC Cyber Center recommends remaining vigilant for phishing or social engineering attempts conducted through URLs, websites, emails, texts, phone calls, voicemails, social media, or alternative messaging platforms and encourages the use of lengthy, complex, and unique passwords for each account. We urge users to enable multifactor authentication when available to avoid falling victim to account compromise. Additionally, avoid opening unexpected correspondence and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. Never provide sensitive and personal information in response to unsolicited correspondence. If you believe you have been targeted by a malicious campaign or had credentials or personal information compromised, notify the relevant IT security teams immediately. Please see the NTIC Cyber Center’s product [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

Malware Campaigns

SUPERNOVA Malware Likely Leveraged via SolarWinds Flaw

An authentication bypass vulnerability in the SolarWinds Orion software may have been [leveraged](#) by adversaries as a zero-day to deploy the SUPERNOVA malware in target environments. According to an advisory published yesterday by the CERT Coordination Center, the SolarWinds Orion API that’s used to interface with all other Orion system monitoring and management products suffers from a security flaw (CVE-2020-10148) that could allow a remote attacker to execute unauthenticated API commands, thus resulting in a compromise of the SolarWinds instance.

Gift Card Phishing Campaign Delivers Dridex Malware

The Dridex malware gang is [delivering](#) a nasty gift for the holidays using a spam campaign pretending to be Amazon Gift Cards. Dridex is a modular banking trojan that can perform various malicious activities, including stealing login information, logging keystrokes, taking screenshots, and downloading and installing further malware. The Dridex gang’s new emails pretend to be a \$100 gift certificate that users must redeem by clicking on a link. When the button is clicked, it will download malicious Word documents with names similar to “Amazon_Gift_Card,” “Order_Gift_Cart,” and “Amazon_eGift-Card.” The Word documents state that they were created in an online version of Microsoft Office and prompt the recipient to click on the “Enable Content” button. Doing so will execute malicious macros that downloads and installs the Dridex malware, and possibly other payloads, on the victim’s computer.

The NTIC Cyber Center recommends maintaining regular system backups; monitoring network traffic for suspicious activity; securing connection services; and keeping all devices, applications, antivirus platforms, and operating systems patched and up-to-date. We also recommend decommissioning any unsupported or end-of-life (EOL) systems and software. In addition, users should avoid using domain-wide, administrator-level service accounts and avoid clicking on unknown links in correspondence and downloading content from untrusted sources. We encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication when available to avoid account compromise. To improve your organization’s cybersecurity posture, we encourage you to review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with “Unsubscribe” in the subject line and you will immediately be removed from our distribution list.

Securing Our Communities

Each week, the NTIC Cyber Center highlights a different social engineering scam impacting individuals and communities within the National Capital Region. We encourage everyone to share this information with friends, colleagues, and loved ones to reduce their risk of becoming a victim of financial fraud and identity theft.



Peer-to-Peer (P2P) payment scams are schemes in which perpetrators elicit money from victims via P2P payment apps. With just a mobile number or email address connected to a financial account, P2P payment apps allow transactions to be made easily and immediately between individuals and can be used to split bills such as bar tabs or housing expenses. These apps are available for download onto smartphones, tablets, and smartwatches. Although there are very legitimate uses for these apps, scammers have targeted P2P payment app users for financial gain and to steal login credentials or install malware on users' devices. Read [this](#) NTIC Cyber Center report to learn about this prevalent scam and how to protect yourself.

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

WEEKLY CYBER THREAT DIGEST

12 February 2020

Product No. 2020-02-016
NTIC SIN No. 2.5 | HSEC SIN No. 1

Emerging Cyber Threats & Trends

Threat Actors Exploit Social Media Data

Every photo that is posted, status that is updated, person that is tagged, and place that gets checked into on social media [reveals](#) valuable information about our personal and professional lives. Hackers use this information to craft targeted, believable, and — most importantly — effective social engineering attacks against people and businesses. These attacks leave PII, trade secrets, and money vulnerable to exploitation. If a social media account is public, if photos are shared, and if family and friends are linked to the account, this information is surprisingly easy to uncover. One-third of people share business travel updates and photos online and 93% of users update their social media profiles when they get a new job. This can help hackers decide who to impersonate, who to target (people with new jobs can be prime targets), when to target them, and what penetration means to use for the attack.

Data Leaks and Breaches

Children's Health Insurer's Website Vulnerable for 7 Years

Florida Healthy Kids learned that its web hosting vendor failed to [apply](#) security patches to its software, thereby exposing the website to vulnerabilities that were ultimately exploited by hackers. The vulnerabilities spanned a seven-year period from November 2013 until December 2020. The organization temporarily shut down its website and databases in December 2020. The organization released a statement saying, "The Florida KidCare online application will remain down until it is restored by our new web hosting vendor." Individuals' full names, dates of birth, email addresses, phone numbers, physical addresses, social security numbers, and financial information may have been exposed.

Threat Actors Briefly Gain Access to US Town's Water Supply

While the attack on a Florida water treatment plant was [thwarted](#), hackers remotely gained access to a software program, TeamViewer, via an employee's computer and gained control of the plant's systems, according to the sheriff of Oldsmar, Florida. The hackers were able to increase the amount of sodium hydroxide, also known as lye, being injected into the water supply. The water treatment facility detected and quickly reversed the command before incurring any impact to the public water supply. Sodium hydroxide is typically used in small amounts to control the acidity of water, but it is dangerous at higher levels. TeamViewer, has been installed on 2.5 billion devices worldwide, and enables remote technical support. The FBI and Secret Service are assisting in the investigation; those responsible for the cyberattack have not been identified.

The NTIC Cyber Center recommends affected consumers apply for free credit monitoring services if offered by the compromised company; monitor bank and credit card statements closely; immediately report any unauthorized activity to their financial institutions; ensure new passwords are lengthy, complex, and unique to each account; and enable multifactor authentication when available. Victims of this or other data breaches are encouraged to visit the Federal Trade Commission's online [identity theft resource page](#) and consider placing a fraud alert or security freeze on their credit file.

Phishing Campaigns

COVID-19 Vaccine Scams Appearing Online

Check Point has recorded thousands of website domains recently registered with phrases including "vaccine" and "corona". In a related [study](#), Interpol found that, out of a sample of 3,000 websites appearing to sell dubious medicine and medical devices, roughly 1,700 contained cyber threats including phishing code and malware. Never purchase medical equipment or treatments from unofficial, untrusted sources. Cybercriminals do not care what sale vector must be used to make a profit and are likely to exploit demand for life-saving vaccines. These criminals' tactics, techniques and procedures (TTP) include sending out fraudulent emails, fake online advertisements related to the COVID-19 outbreak or vaccine, COVID-19-related fraudulent texts, and cold calling victims directly.

Increase in OAuth Phishing Attacks Against Microsoft Office 365

Microsoft has [warned](#) of an increasing number of consent phishing (also known as OAuth phishing) attacks targeting remote workers during recent months. OAuth phishing is an application-based attack variant where the attackers trick targets into providing malicious Office 365 OAuth apps (web apps registered by the attackers with an OAuth 2.0 provider) with access to their Office 365 accounts. Once victims grant the malicious apps access to their account's data, the threat actors exploit their permissions and refresh tokens, enabling them to take over the Microsoft accounts and make API calls through the attacker-controlled Office 365 OAuth app. The compromised Office 365 accounts provide the attackers with access to victims' emails, files, contacts, as well as sensitive information and resources stored on corporate SharePoint document management/storage systems and/or OneDrive for Business cloud storage spaces.

The NTIC Cyber Center recommends remaining vigilant for phishing or social engineering attempts conducted through URLs, websites, emails, texts, phone calls, voicemails, social media, or alternative messaging platforms and encourages the use of lengthy, complex, and unique passwords for each account. We urge users to enable multifactor authentication when available to avoid falling victim to account compromise. Additionally, avoid opening unexpected correspondence and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. Never provide sensitive and personal information in response to unsolicited correspondence. If you believe you have been targeted by a malicious campaign or had credentials or personal information compromised, notify the relevant IT security teams immediately. Please see the NTIC Cyber Center's product [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

Malware Campaigns

Cerber Ransomware Used to Target Healthcare Providers

A form of ransomware that was once the most [popular](#) choice among cyber criminals has made a comeback and is being used to target healthcare: Cerber ransomware. The potency of Cerber has resulted in countless victims giving in to ransom demands, providing a profitable business model for both Cerber authors and affiliates. Analysis of 239 million attempted cyberattacks targeting healthcare customers found Cerber to be the most common form of ransomware, accounting for 58% of ransomware attacks targeting the sector. Cerber might be one of the older forms of ransomware, but the prolific way it's being distributed by phishing emails and compromised websites suggests that it is still effective. A senior cybersecurity strategist at VMware Carbon Black explains, "Although old malware variants such as Cerber tend to resurface, these are often re-factored to include new tricks, though at the core are still leveraging tried and true techniques."

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Android Barcode Scanner App Compromised Millions of Users

Lavabird Ltd.'s Barcode [Scanner](#) is an Android app that was available on Google's Play Store for years. The app, that was installed over 10 million times, offered a QR code reader and a barcode generator. The mobile application appeared to be a legitimate, trustworthy software; many users installed the app years ago without any problems until recently. A software update issued around December 4, 2020 changed the functions of the app to push advertising to phones without warning. While many developers implement ads in their software in order to offer free versions, the shift of apps from useful resources to adware has become more common. Malwarebytes reported Lavabird's update to Google, which has now pulled the app from Google Play. However, this doesn't mean that the app will vanish from impacted devices, so users need to manually uninstall the now-malicious app.

The NTIC Cyber Center recommends maintaining regular system backups; monitoring network traffic for suspicious activity; securing connection services; and keeping all devices, applications, antivirus platforms, and operating systems patched and up-to-date. We also recommend decommissioning any unsupported or end-of-life (EOL) systems and software. In addition, users should avoid using domain-wide, administrator-level service accounts and avoid clicking on unknown links in correspondence and downloading content from untrusted sources. We encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication when available to avoid account compromise. To improve your organization's cybersecurity posture, we encourage you to review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

WEEKLY CYBER THREAT DIGEST

19 February 2020

Product No. 2020-02-022
NTIC SIN No. 2.5 | HSEC SIN No. 1

Emerging Cyber Threats & Trends

Attacks on Healthcare Systems and Databases

The healthcare industry is plagued by a myriad of cybersecurity-related [issues](#). These issues range from malware that compromises the integrity of systems and privacy of patients to distributed denial of service (DDoS) attacks that disrupt facilities' ability to provide patient care. While other critical infrastructure sectors experience these attacks as well, the nature of the healthcare industry's mission poses unique challenges. For healthcare, cyberattacks can have ramifications beyond financial loss and breach of privacy. They are also becoming increasingly common. Analyzing data from the U.S. Department of Health and Human Services, threat protection company Bitglass [found](#) that the count of healthcare breaches reported in 2020 increased to 599, a jump of more than 50% compared to the previous year, when there were 386 breaches.

Data Leaks and Breaches

Millions of Amazon and eBay Account Details Allegedly Sold Online

An unknown user posted on a popular hacking forum that s/he was [selling](#) the data of 14 million Amazon and eBay customers' accounts for sale on a popular hacking forum. The leaked data included the customer's full name, postal code, delivery address, and shop name, as well as 1.6 million phone records. The post author has since closed the sale, after two copies were reportedly sold. The data of users appears to come from users who had Amazon or eBay accounts from 2014-2021 in 18 different countries. The data is sorted by country, and the database was being sold for \$800. At the moment, it is unclear how the threat actor acquired the data. It appears that neither Amazon nor eBay suffered any breaches on their end. The threat actor likely used a popular method of password spraying to acquire these credentials.

The NTIC Cyber Center recommends affected consumers apply for free credit monitoring services if offered by the compromised company; monitor bank and credit card statements closely; immediately report any unauthorized activity to their financial institutions; ensure new passwords are lengthy, complex, and unique to each account; and enable multifactor authentication when available. Victims of this or other data breaches are encouraged to visit the Federal Trade Commission's online [identity theft resource page](#) and consider placing a fraud alert or security freeze on their credit file.

Phishing Campaigns

Phishers use Fake LinkedIn Private Shared Document as Lures

Phishers are trying to [trick](#) users into opening a "LinkedIn Private Shared Document" and entering their login credentials into a fake LinkedIn login page. The phishing message is delivered via LinkedIn's internal messaging system and looks like it has been sent by one of the victim's contacts. The message urges the recipient to follow a third-party link to view a document. There is no such thing as a "LinkedIn Private Shared Document," and if recipients fail to vet these lures, they will be redirected to a convincingly spoofed LinkedIn login page. If the recipient enters their login credentials, their account will probably soon be sending out phishing messages to their contacts.

The NTIC Cyber Center recommends remaining vigilant for phishing or social engineering attempts conducted through URLs, websites, emails, texts, phone calls, voicemails, social media, or alternative messaging platforms and encourages the use of lengthy, complex, and unique passwords for each account. We urge users to enable multifactor authentication when available to avoid falling victim to account compromise. Additionally, avoid opening unexpected correspondence and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. Never provide sensitive and personal information in response to unsolicited correspondence. If you believe you have been targeted by a malicious campaign or had credentials or personal information compromised, notify the relevant IT security teams immediately. Please see the NTIC Cyber Center's product [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

Malware Campaigns & Disruption

DoppelPaymer Ransomware is Being Used to Target Kia Motors

Kia Motors America has [suffered](#) a ransomware attack by the DoppelPaymer gang, demanding \$20 million to not leak stolen data and to provide a decryptor. Kia Motors America also has suffered a nationwide IT outage that has affected their mobile UVO Link apps, phone services, payment systems, owner's portal, and internal sites used by dealerships. The reported ransom demand claims that a "huge amount" of data was stolen, or exfiltrated, from Kia Motors America, and it will be released in 2-3 weeks if the company does not negotiate with the threat actors. DoppelPaymer is demanding 404 bitcoins in payment – equivalent to approximately \$20 million. If the ransom is not paid within a specific time frame, the amount will increase to 600 bitcoins, or approximately \$30 million. The DoppelPaymer operation has not indicated what type of data has been stolen. Based on the amount of Kia services that suffered outages, the DoppelPaymer operation may have stolen information from a wide range of servers.

Telephony Denial-Of-Service Attacks Can Lead to Loss of Lives

The Federal Bureau of Investigation (FBI) has [warned](#) of the harsh consequences of telephony denial-of-service (TDoS) attacks and has provided recommended steps to mitigate their impact. The FBI published this warning on Wednesday as an [IC3 public service announcement](#) and as a Private Industry Notification issued to private sector organizations in coordination with DHS-CISA. TDoS attacks are manual or automated malicious attempts to render telephone systems unavailable by blocking incoming and outgoing calls, which could have dire consequences when directed at 911 or similar emergency call center operations. As the FBI noted in yesterday's warning, malicious actors provide TDoS services and tools to attackers with varying levels of experience, which drastically lowers the skill level needed to launch such attacks. TDoS attacks are challenging to detect, given that attackers spoof the caller ID on every call (in some cases spoofing the phone numbers of police departments.) This makes it almost impossible to differentiate between malicious and legitimate calls.

The NTIC Cyber Center recommends maintaining regular system backups; monitoring network traffic for suspicious activity; securing connection services; and keeping all devices, applications, antivirus platforms, and operating systems patched and up-to-date. We also recommend decommissioning any unsupported or end-of-life (EOL) systems and software. In addition, users should avoid using domain-wide, administrator-level service accounts and avoid clicking on unknown links in correspondence and downloading content from untrusted sources. We encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication when available to avoid account compromise. To improve your organization's cybersecurity posture, we encourage you to review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

WEEKLY CYBER THREAT DIGEST

26 February 2021

Product No. 2020-02-027
NTIC SIN No. 2.5 | HSEC SIN No. 1

Emerging Cyber Threats & Trends

100K+ Cyber Threats Detected Per Minute

The number of cyber-threats [identified and blocked](#) by Trend Micro rose by 20% in 2020 to more than 62.6 billion. That is an average of 119,000 cyber threats per minute. Email-mediated threats such as phishing attacks accounted for 91% of the 62.6 billion threats. Nearly 14 million unique phishing URLs were detected by the company in 2020; home networks were the primary target. Researchers found cyber attacks on home networks surged 210% in 2020 to just under 2.9 billion. The vast majority of strikes against home networks involved brute-forcing logins to gain control of a smart device or router. In addition, there were 34% more newly detected ransomware families last year. Researchers noted an increase in the popularity of “double extortion” attacks: attackers exfiltrate data before encrypting it so they can use the threat of publication to extort money as well as charging for the data's return. Government, banking, manufacturing, and healthcare were the sectors most targeted by ransomware gangs. Some flaws exploited by criminals date back to 2005.

Data Leaks and Breaches

12,000 Daycare Webcam Service User Accounts Exposed

NurseryCam, a webcam service used for baby monitoring across 40 daycare centers in the U.K., [has shut down](#) following a data breach. An attacker who claimed to be trying to improve the service's security was able to find a “loophole” in the system's security. NurseryCam was alerted to the breach last Friday afternoon, and sent a notice to its users. By Saturday, the NurseryCam service was shut down while a fix was being applied. The hacker claimed they were able to get real names, usernames, email addresses, and encrypted passwords for 12,000 accounts. The director of NurseryCam does not believe anyone watched the webcams without permission; rather, the person behind the breach contacted the company to report the incident. “He stated he has no intention to use this to do any harm [and] wants to see NurseryCam raise the overall standards of our security measures,” she said.

The NTIC Cyber Center recommends affected consumers apply for free credit monitoring services if offered by the compromised company; monitor bank and credit card statements closely; immediately report any unauthorized activity to their financial institutions; ensure new passwords are lengthy, complex, and unique to each account; and enable multifactor authentication when available. Victims of this or other data breaches are encouraged to visit the Federal Trade Commission's online [identity theft resource page](#) and consider placing a fraud alert or security freeze on their credit file.

Phishing Campaigns

Microsoft Users Targeted by Fake FedEx and DHL Emails

Researchers are [warning](#) of recent phishing attacks targeting at least 10,000 Microsoft email users; the phishing scams are posing as popular mail couriers FedEx and DHL Express. Both scams have targeted Microsoft email users and have aimed to swipe users' work email account credentials. The attackers have used phishing pages hosted on legitimate domains, allowing the emails to slip by security filters built to block known bad links. "The email titles, sender names, and content did enough to mask their true intention and make victims think the emails were really from FedEx and DHL Express respectively," said researchers with Armorblox. "Emails informing us of FedEx scanned documents or missed DHL deliveries are not out of the ordinary; most users will tend to take quick action on these emails instead of studying them in detail for any inconsistencies."

The NTIC Cyber Center recommends remaining vigilant for phishing or social engineering attempts conducted through URLs, websites, emails, texts, phone calls, voicemails, social media, or alternative messaging platforms and encourages the use of lengthy, complex, and unique passwords for each account. We urge users to enable multifactor authentication when available to avoid falling victim to account compromise. Additionally, avoid opening unexpected correspondence and refrain from clicking on links, opening attachments, or enabling macros in documents from unknown or untrusted sources. Never provide sensitive and personal information in response to unsolicited correspondence. If you believe you have been targeted by a malicious campaign or had credentials or personal information compromised, notify the relevant IT security teams immediately. Please see the NTIC Cyber Center's product [Securing Our Communities: How to Identify Phishing Emails and Avoid Becoming a Victim](#).

Malware Campaigns & Disruption

30,000 Macs Infected with New Malware

Security researchers have [spotted](#) a new malware operation targeting Mac devices that has silently infected almost 30,000 systems. Once an hour, infected Macs check a control server to see if there are any new commands the malware should run or binaries the malware should execute. So far, researchers have yet to observe delivery of any payload on any of the infected 30,000 machines, leaving the malware's ultimate goal unknown. The lack of a final payload suggests that the malware may spring into action once an unknown condition is met. The malware also comes with a mechanism to completely remove itself, a capability that's typically reserved for high-stealth operations. So far, there are no signs the self-destruct feature has been used. The malware is notable for running natively on the M1 chip that Apple introduced in November, making it only the second known piece of macOS malware to do so. The malware has been found in 153 countries and is most highly concentrated in the US, UK, Canada, France, and Germany. Its use of Amazon Web Services and the Akamai content delivery network ensures that the command infrastructure works reliably and that the servers are difficult to block.

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Supply Chain Hack (SolarWinds) Took A Thousand Engineers to Pull Off, Tech Exec Tells Congress

The president of Microsoft [told](#) a panel of U.S. Senators on Tuesday that his company estimates the cybersecurity breach of nine federal agencies and 100 private companies likely took "at least a thousand" skilled and capable people to pull off. The scope and scale described is consistent with the attribution made by public and private sector officials that the hack, which leveraged flaws in IT management software from SolarWinds to inject malware into computer networks, was perpetrated by nation-state sponsored actors. FireEye, the firm credited with discovering the initial breach has stated that the hack was likely the work of a state or state-sponsored actor. The *Washington Post* [reported](#) on Tuesday that the White House is planning to sanction Russia in response to the SolarWinds espionage campaign, a range of malign cyberactivity, and the near-fatal poisoning of a Russian opposition leader. The *Post*'s reporting also added NASA and the Federal Aviation Administration to the list of agencies compromised.

The NTIC Cyber Center recommends maintaining regular system backups; monitoring network traffic for suspicious activity; securing connection services; and keeping all devices, applications, antivirus platforms, and operating systems patched and up-to-date. We also recommend decommissioning any unsupported or end-of-life (EOL) systems and software. In addition, users should avoid using domain-wide, administrator-level service accounts and avoid clicking on unknown links in correspondence and downloading content from untrusted sources. We encourage the use of lengthy, complex, and unique passwords for each account and enabling multifactor authentication when available to avoid account compromise. To improve your organization's cybersecurity posture, we encourage you to review our free Ransomware Mitigation and Cyber Incident Response Planning guides, available on our [website](#).

T L P : W H I T E

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

Disclaimer: The NTIC Cyber Center Weekly Cyber Threat Bulletin is provided for informational purposes only. The NTIC Cyber Center does not endorse any commercial vendor, product, or service referenced in this email or otherwise. Further dissemination of this email is governed by the Traffic Light Protocol (TLP). For more information about TLP designations, please visit [US-CERT](#).

You are receiving this email because you have previously requested cybersecurity products from the NTIC, either by submitting an NTIC NDA, signing up on our [website](#), or by sending us an email asking to receive our products. To stop receiving our emails, please reply with "Unsubscribe" in the subject line and you will immediately be removed from our distribution list.

Q29 HSEMA

TOP 25 - FY 2020 OVERTIME EARNERS BY EMPLOYEE

Agency Code	Fiscal Year	Program Number	Activity Number	Employee Name	Position Number	Position Title	Salary	Fringe	Overtime Pay
BNO	20	1000	1325	Ruesch, Emily	92023	Program Coordinator (State)	137,255.00	31,431.40	51,954.01
BNO	20	3000	3402	Hauser, Eric	28225	Logistics Management Specialis	95,111.00	21,780.42	49,669.23
BNO	20	2000	2113	Cryan, Travis	1055	Emergency Exer. & Trng. Spec.	95,111.00	21,780.42	46,428.22
BNO	20	2000	2103	Stewart, Jonathan	77972	Training and Emergency Exer cis	149,350.00	34,201.15	38,791.67
BNO	20	1000	1325	Bernet, Courtney Graf	88691	Emergency Planning Specialist	102,782.00	23,537.08	38,622.94
BNO	20	3000	3402	Harris, Jason Burrell	85181	Logistics Management Specialis	89,997.00	20,609.31	36,175.72
BNO	20	4000	4100	Coleman, Bettina R	48762	Grants Program Manager	110,063.00	25,204.43	33,038.74
BNO	20	1000	1325	Mc Dermott, Nicole M	2939	Program Analyst	79,314.00	18,162.91	32,687.28
BNO	20	3000	3100	Scott II, Renaud D.	75240	Deputy Chief of Operations	129,411.00	29,635.12	31,419.50
BNO	20	1000	1320	Shackelford, Jerica D	71851	Supv Mgmt and Program Analyst	140,000.00	32,060.00	30,624.49
BNO	20	3000	3100	Franklin, Carolyn	16080	STAFF ASSISTANT	100,225.00	22,951.52	29,344.73
BNO	20	3000	3100	Rodgers Jr., Billy F.	19500	Emergency Operations&Info Spec	75,094.00	17,196.52	29,323.23
BNO	20	3000	3402	Woodall, Kenneth	75239	Supv Mgmt and Program Analyst	140,080.00	32,078.32	28,218.04
BNO	20	4000	4100	Reed, Tristan F	45279	Grants Management Officer	129,410.75	29,635.06	27,624.21
BNO	20	2000	2313	Williams, Ladona R.	44868	Emergency Planning Specialist	67,578.00	15,475.36	25,666.62
BNO	20	4000	4305	Bazel, Nicolette D	94954	Staff Assistant	85,570.00	19,595.53	25,126.79
BNO	20	3000	3113	Jachimowicz, Adam Mark	92021	Program Coordinator (State)	120,257.00	27,538.85	24,571.74
BNO	20	4000	4305	Plavan, Timur	18601	Supervisory IT Specialist	109,262.40	25,021.08	23,311.34
BNO	20	4000	4305	Cherinet, Hirut A	95151	Information Technology Spec.	92,554.00	21,194.87	23,221.57
BNO	20	3000	3100	Lucas, Donte O	88525	Deputy Chief of Operations	129,854.16	29,736.60	23,070.00
BNO	20	2000	2106	Goodman, Anthony T.	77540	PGM ANALYST	122,227.00	27,989.98	23,005.72
BNO	20	4000	4305	Lescure, William	85184	Geographic Information Systems	107,022.00	24,508.04	22,446.42
BNO	20	2000	2100	Alsop, Vernecia R	48765	Grants Program Manager	110,063.00	25,204.43	22,171.35
BNO	20	4000	4305	El Baamrani, Hamid	95150	Information Technology Spec.	92,554.00	21,194.87	22,169.07
BNO	20	1000	1320	Wilson, Larae Mechelle	88355	Emergency Operations&Info Spec	83,646.00	19,154.94	21,620.02
AGENCY GRAND TOTAL							\$2,693,791.31	\$616,878.21	\$760,302.65

TOP 25 - FY 2021 OVERTIME EARNERS BY EMPLOYEE

Agency Code	Fiscal Year	Program Number	Activity Number	Employee Name	Position Number	Position Title	Salary	Fringe	Overtime Pay
BNO	20	1000	1325	Ruesch, Emily	00092023	Program Coordinator (State)	137,255.00	31,431.40	14,451.37

BN0	20	3000	3363	Guddemi, Charles	00048775	Statewide Communications Inter	144,439.00	33,076.53	14,426.55
BN0	20	3000	3111	Mc Dermott, Nicole M	00002939	Program Analyst	79,314.00	18,162.91	10,486.24
BN0	20	3000	3111	Lucas, Donte O	00088525	Deputy Chief of Operations	129,854.16	29,736.60	9,239.64
BN0	20	2000	2103	Goodman, Anthony T.	00077540	PGM ANALYST	122,227.00	27,989.98	7,977.06
BN0	20	1000	1306	Mena, Rebekah J.	00085113	Program Analyst	97,375.00	22,298.88	7,548.89
BN0	20	3000	3111	Farley, James J.	00019028	Emergency Planning Specialist	75,094.00	17,196.53	6,367.29
BN0	20	2000	2113	Cryan, Travis	00001055	Emergency Exer. & Trng. Spec.	95,111.00	21,780.42	6,173.08
BN0	20	1000	1310	Adams, Nikelle L.	00075241	Program Analyst	95,111.00	21,780.42	5,761.52
BN0	20	5000	5182	Marcenelle, Madeline	00077728	Supervisory Intelligence Analy	120,500.00	27,594.50	5,329.81
BN0	20	2000	2100	Alsop, Vernecia R	00048765	Grants Program Manager	113,104.00	25,900.82	5,057.05
BN0	20	3000	3402	Hauser, Eric	00028225	Logistics Management Specialis	95,111.00	21,780.42	5,007.05
BN0	20	2000	2103	Williams, Ladona R.	00044868	Emergency Planning Specialist	67,578.00	15,475.36	4,873.41
BN0	20	3000	3100	Wiggins Sr., Brian	00010514	Emergency Operations&Info Spec	75,094.00	17,196.53	4,434.46
BN0	20	1000	1310	Mitchell, Tanya L	00012886	Emergency Management Program O	130,217.00	29,819.69	4,225.79
BN0	20	3000	3100	Hackney, David	00007419	EMERGENCY OPERATION INFO SPEC	81,508.00	18,665.33	4,169.44
BN0	20	3000	3111	Partridge, Nathaniel Steven	00097267	Emergency Planning Specialist	71,106.00	16,283.27	4,076.63
BN0	20	1000	1320	Shackelford, Jerica D	00071851	Supv Mgmt and Program Analyst	140,000.00	32,060.00	3,971.15
BN0	20	4000	4100	Reed, Tristan F	00045279	Grants Management Officer	129,410.75	29,635.06	3,919.67
BN0	20	5000	5182	Spalding, Jordan	00097266	Fusion Intelligence Analyst	72,956.00	16,706.92	3,788.10
BN0	20	4000	4FA1	Huggins, Briana	00007908	PGM ANALYST	100,940.00	23,115.26	3,785.25
BN0	20	3000	3100	Goldsmith, Frederick W.	00026092	Deputy Chief of Operations	128,176.88	29,352.51	3,697.40
BN0	20	3000	3100	Sneed Jr., Robert W	00023961	Deputy Chief of Operations	110,376.04	25,276.11	3,661.49
BN0	20	5000	5183	Randolph, Sedley A	00047136	Fusion Intelligence Analyst	62,286.00	14,263.49	3,510.92
BN0	20	5000	5182	Lambert, Jordan J.	00085179	Fusion Intelligence Analyst	89,997.00	20,609.31	3,504.68
AGENCY GRAND TOTAL							\$2,564,140.83	\$587,188.25	\$149,443.94

WORKING CONDITIONS AGREEMENT

BETWEEN

**DISTRICT OF COLUMBIA GOVERNMENT
HOMELAND SECURITY AND EMERGENCY
MANAGEMENT AGENCY**

AND

**NATIONAL ASSOCIATION OF GOVERNMENT
EMPLOYEES/SERVICE EMPLOYEES
INTERNATIONAL UNION,
LOCAL R3-08**

EFFECTIVE

OCTOBER 1, 2014 THROUGH SEPTEMBER 30, 2017

TABLE OF CONTENTS

PREAMBLE	1
ARTICLE 1 RECOGNITION	1
ARTICLE 2 MANAGEMENT RIGHTS AND RESPONSIBILITIES.....	2
ARTICLE 3 LABOR-MANAGEMENT COOPERATION	3
ARTICLE 4 NON-DISCRIMINATION	4
ARTICLE 5 EMPLOYEE LISTS AND INFORMATION	6
ARTICLE 6 POSITION MANAGEMENT AND CLASSIFICATION	6
ARTICLE 7 TRAINING CAREER DEVELOPMENT AND UPWARD MOBILITY	7
ARTICLE 8 SAFETY AND HEALTH	8
ARTICLE 9 PERSONNEL FILES	12
ARTICLE 10 DISTRIBUTION OF AGREEMENT AND ORIENTATION OF EMPLOYEES.....	13
ARTICLE 11 PROBATIONARY EMPLOYEES.....	14
ARTICLE 12 REORGANIZATION/REALIGNMENT	14
ARTICLE 13 GOVERNING LAWS AND REGULATIONS	15
ARTICLE 14 EMPLOYEE RIGHTS	15
ARTICLE 15 BULLETIN BOARDS.....	16
ARTICLE 16 UNION REPRESENTATIONS.....	16
ARTICLE 17 UNION SECURITY AND UNION DUES DEDUCTIONS.....	19
ARTICLE 18 CONTRACTING OUT	20
ARTICLE 19 VACANCY ANNOUNCEMENTS	21
ARTICLE 20 REDUCTION IN FORCE	21
ARTICLE 21 SCHEDULING/ HOURS OF WORK	22
ARTICLE 22 ADMINISTRATION OF LEAVE	23
ARTICLE 23 DISCIPLINE	26
ARTICLE 24 GRIEVANCE/ARBITRATION PROCEDURES.....	28
ARTICLE 25 DISTRICT PERSONNEL MANUAL	35
ARTICLE 26 FACILITIES AND SERVICES.....	35
ARTICLE 27 DETAILS AND TEMPORARY PROMOTIONS	36
ARTICLE 28 SAVINGS CLAUSE	37
ARTICLE 29 CAREER LADDER	37
ARTICLE 30 NEW TECHNOLOGY	38

ARTICLE 31 SENIORITY.....38

ARTICLE 32 ADMINISTRATIVE OF OVERTIME39

ARTICLE 33 DURATION AND FINALITY.....40

APPENDIX 1 EXCHANGE OF WORK DAYS FORM.....42

APPENDIX 2 OFFICIAL TIME REPORT44

PREAMBLE

This Agreement is entered into between the Homeland Security and Emergency Management Agency (hereinafter referred to as the Agency or HSEMA) and the National Association of Government Employees/Service Employees International Union, Local R3-08 (Hereinafter referred to as the Union or NAGE), and collectively known as the Parties.

The Parties to this Agreement hereby recognize that the collective bargaining relationship reflected in this agreement is of mutual benefit and the result of good faith collective bargaining between the parties. Further, all parties agree to establish and promote a sound and effective labor-management relationship in order to achieve mutual understanding of practices, procedures and matters affecting conditions of employment and to continue working toward this goal.

The Parties hereto affirm without reservation the provisions of this agreement, and agree to honor and support the commitments contained herein. The parties agree to resolve the differences that may arise between them through the dispute resolution processes agreed to through negotiations of this Agreement.

The purpose of this Agreement is:

1. to promote fair and reasonable working conditions;
2. to promote harmonious relations between the parties;
3. to establish an equitable and orderly procedure for the resolution of differences;
4. to protect the rights and interests of the employee, the Union and the Agency;
5. to improve the morale of employees in service to the District of Columbia; and
6. to promote the efficient and professional operations of the Agency.

It is the intent and purpose of the parties hereto to promote and improve the efficiency and quality of service provided by the Agency. Therefore, in consideration of mutual covenants and promises contained herein, HSEMA and the Union do hereby agree as follows:

ARTICLE 1 **RECOGNITION**

Section A:

1. The National Association of Government Employees/Service Employees International Union, Local R3-08, is hereby recognized as the sole and exclusive representative for all employees in the bargaining unit as described in Section B of this Article.

2. The Union, as the exclusive representative of all employees in the unit, has the right, as provided in D.C. Official Code §§1-617.01 through 1-617.17 (2001 Ed.), to negotiate agreements covering all employees in the unit and is responsible for representing the interests of all such employees without discrimination and without regard to membership in the labor organization.

Section B:

The HSEMA bargaining unit represented by the Union is as follows:

All employees of the Homeland Security and Emergency Management Agency including Emergency Operations and Information Specialist, Emergency Operations and information Specialist Bilingual, Emergency Operations VIP Technicians, all other clerical employees, excluding managers, supervisors, confidential employees, and employees engaged in personnel work other than in a purely clerical capacity and employees engaged in administering the provisions of Title XVII of the District of Columbia Comprehensive Merit Personnel Act of 1978, D.C. Law 2-139.

PERB Case No. 10-RC-01, Certification No. 152 (2011).

Section C:

Nothing in this Article shall be construed as a waiver of any Agency or Union right.

ARTICLE 2
MANAGEMENT RIGHTS AND RESPONSIBILITIES

Section A:

The sole rights of management are prescribed in the Comprehensive Merit Personnel Act (CMPA) under D.C. Official Code § 1-617.08 (2001 Ed.) and shall be recognized in accordance with the CMPA.

Section B:

All matters shall be deemed negotiable except those that are proscribed by D.C. Official Code § 1-617.08 and decisions issued by the Public Employee Relations Board as a result of negotiability petition appeals.

Section C:

This article shall not preclude the Union's right to bargain, upon request, over the impact and effect of decisions made pursuant to D.C. Official Code § 1-617.08.

ARTICLE 3
LABOR-MANAGEMENT COOPERATION

Section A:

Consistent with the principles of the D.C. Labor-Management Partnership Council, the parties agree to establish and support appropriate partnerships within the HSEMA. The labor-management cooperation committee shall be composed of equal number of high level officials representing each Party. The purpose of the meeting shall be to discuss different points of view and exchange views on working conditions, terms of employment, matters of common interest or other matters which either Party believes will contribute to improvement in the relations between them within the framework of this Agreement. It is understood that appeals, grievances or problems of individual employees shall not be subjects of discussion at these meetings, nor shall the meeting be for any other purpose which will modify, add to or detract from the provisions of this Agreement.

Section B:

The committee shall establish itself within 30 days of signing and approval of this Agreement and shall request partnership training within 60 days of establishing itself. Such training shall be conducted on a bi-annual basis. The parties shall make every attempt to have Federal Mediation and Conciliation Services (hereinafter referred to as the "FMCS") provide such training. Any cost associated with partnership training shall be shared equally by the Parties. The LMPC shall determine its guidelines and operating procedures at its inaugural meeting and memorialize such procedures in writing. All committee decisions shall be made by consensus only.

Section C:

1. The standing members of the LMPC appointed by the Union shall be granted official time to attend the LMPC meetings. If such member(s) attend(s) a meeting that falls outside of his or her normal tour of duty, the Agency shall modify their tour of duty. If the employee's tour of duty cannot be modified, the meeting will be rescheduled.
2. The Union shall notify the Agency at least one (1) day in advance of any scheduled meeting if an alternate will attend in the absence of the appointed member. The Agency shall grant official time to the alternate member.

Section D:

If issues of health and/or safety arise, either Party may demand a meeting of the committee of all or part of the committee to be scheduled as soon as is practicable.

ARTICLE 4
NON-DISCRIMINATION

Section A:

In accordance with the D.C. Human Rights Act of 1977, as amended, D.C. Official Code §2-1401.01 *et seq.*, (Act), the Agency and the Union agree not to discriminate for or against employees covered by this Agreement on account of membership or non-membership in the Union, or on the basis of: race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, familial status, family responsibilities, gender identity or expression, matriculation, political affiliation, disability, genetic information, source of income, or place of residence or business. Sexual harassment is a form of sex discrimination which is prohibited by the Act. In addition, harassment based on any of the above protected categories is prohibited. Discrimination in violation of the Act will not be tolerated. Violators may be subject to disciplinary action.

Section B:

1. The agency agrees to implement its personnel management policies, procedures or practices in accordance with EEO procedures and statutes, and the Union shall, upon request be permitted to meet with Agency EEO officials to discuss these, including reasonable accommodations to the religious needs of employees.
2. The parties agree that EEO complaints shall be processed in accordance with District law, rules and regulations.

Section C:

The agency shall provide the Union annually with its affirmative action plan.

Section D:

The Union recognizes its responsibility as bargaining agent and agrees to represent all employees in the unit without discrimination.

Section E:

The agency agrees that the union may submit names of employees to the agency for consideration for appointment as EEO counselors, using the same criteria that are used for other nominees. The names and telephone numbers of the agency's EEO Counselors shall be posted on the agency's bulletin board. The union shall be promptly notified in writing of the names and telephone numbers of the agency's EEO Counselors.

Section F:

The agency shall ensure that all EEO counselors receive training through the D.C. Office of Human Rights.

Section G:

1. The Agency and the Union recognize that sexual harassment is a form of misconduct that undermines the integrity of the employment relationship and adversely affects employee opportunities. All employees must be allowed to work in an environment free from unsolicited and unwelcome sexual overtures. Sexual harassment is defined in Equal Employment Opportunity rules governing complaints of discrimination in the District of Columbia Government (31 DCR 56):

"Sexual harassment" means unwelcome sexual advance, requests for sexual favors, and other verbal or physical conduct of a sexual nature when:

- (1) Submission to such conduct is made either explicitly or implicitly a term or condition of employment;
- (2) Submission to or rejection of such conduct by an employee is used as the basis for employment decisions affecting such employee; or
- (3) Such conduct has the purpose of or effect of unreasonably interfering with an employee's work performance or creating an intimidating, hostile or offensive working environment.

2. Sexual harassment may include, but is not limited to:

- a. Verbal harassment or abuse,
- b. Subtle pressure for sexual activity,
- c. Patting or pinching,
- d. Brushing against another employee's body, and
- e. Demands for sexual favors.

Section H:

Alleged violation of EEO rights and obligations in this article are not subject to the grievance and arbitration procedures in this collective bargaining agreement and shall be considered by the appropriate administrative agency having jurisdiction over the matter. This does not preclude the non-EEO aspects of mixed grievances (where a clear distinction can be made and where such complaints are within the scope of the grievance procedure as defined within this agreement) from going through the negotiated procedure.

ARTICLE 5
EMPLOYEE LISTS AND INFORMATION

Section A:

Quarterly, upon request from the Union, the Agency shall, within (5) business days, provide the Union with a list of specific bargaining unit employees or a list of all employees in the bargaining unit, to include the following information:

1. Name;
2. Job title, series and grade;
3. Service Computation Date;
4. "Not to Exceed" dates for term employees; and
5. Appointment status.

Section B:

Quarterly, upon request from the Union, the Agency shall, provide the Union staffing vacancy announcements and a list of bargaining unit members:

1. A list of new hires;
2. Separations;
3. Transfers;
4. Reassignments; and
5. Details in excess of 30 days.

Section C:

Quarterly upon request, the Agency shall provide the Union with an approved, standardized copy of the position description for new or modified bargaining unit positions. The Union shall be given the opportunity to review substantial changes in job descriptions prior to implementation.

ARTICLE 6
POSITION MANAGEMENT AND CLASSIFICATION

Section A:

The Agency endeavors to maintain current and accurate position descriptions. Changes to a position shall be incorporated in the position description to assure that the position is correctly classified and graded to the proper title, series, schedule and grade.

Section B:

Upon request, employees shall be furnished a current, accurate, approved copy of the description of the position to which assigned at the time of assignment, or upon request. Employees detailed or reassigned to established positions shall be given position descriptions at the time of assignment. Employees detailed to an unestablished position shall be furnished with statements of duties at the time of assignment to the detail.

Section C:

In accordance with D.C Code § 1-611.01, the Agency agrees to support the principles of equal pay for equal work. Equal pay for equal work claims may be appealed by the Union through the procedures outlined in the grievance and arbitration provision of this agreement. Classification claims are not subject to the grievance and arbitration provisions of this agreement. Such claims must be appealed through the procedures outlined by District Personnel Manual.

ARTICLE 7
TRAINING, CAREER DEVELOPMENT AND UPWARD MOBILITY

Section A:

Consistent with employee development it is the Agency's intention to provide training and career development opportunities for bargaining unit employees for the purpose of developing and maintaining their skills so that they may perform at the highest possible levels in their positions and advance in accordance with individual potential and abilities.

Section B:

1. The Agency will offer to assist employees in implementing individual career development plans by providing easy access to information on training opportunities, publicizing current training programs, advising employees of requirements needed to enter training programs, scheduling training and making resources available to cover approved expenses for training subject to budgetary considerations.
2. The Agency shall distribute to all bargaining unit employees training programs offered by or through the Agency. The Agency also agrees to publicize external career related training and education opportunities that it is aware of.
3. Employees shall be given reasonable opportunities to discuss training needs and/or opportunities with their supervisors and/or other Agency or Personnel officials.

Section C:

1. Requests for training and educational opportunities shall be acknowledged within 2 days, and processed promptly.
2. A record of satisfactorily completed training courses may be filed by each employee in their Official Personnel File.
3. When an institution of higher learning provides for accreditation of on-the-job experience, upon the employee's request the Agency shall submit verification of such experience.

Section D:

1. The Parties recognize the importance of career development, training and upward mobility. The Labor-Management Committee established in this Agreement shall, on a periodic basis perform the following functions:
 - a. Review existing policies and practices, with respect to training and career development and recommend changes in existing programs;
 - b. Recommend the adoption of new programs, policies and practices; and
 - c. Review and offer comments on programs proposed by the Agency.
2. Any upward mobility plan or recommendations submitted to the Director by the Committee shall be given careful consideration and the Committee shall be informed within a reasonable period of time of the status of its recommendations.

ARTICLE 8
SAFETY AND HEALTH

Section A:

The Agency shall provide the employees with reasonably safe and healthy working conditions in accordance with the D.C. Official Code, §§1-620.01 through 1-620.08 (2001 Ed.). It shall ensure the implementation and enforcement of all applicable District and Federal laws, rules and regulations regarding health and safety. The Union will cooperate in these efforts by encouraging its members to work in a safe manner and to obey established safety practices and regulations.

- a. Protective devices and protective equipment shall be provided by the District and shall be used by all employees when required, unless otherwise deemed unsafe.
- b. Employees shall not be required to work alone in areas where their health and safety would be endangered by working alone.

- c. Employees shall not be required to operate equipment that has been determined unsafe to use when, by doing so, they may injure themselves or others.

Section B:

The Agency shall ensure that training is available, in cardiopulmonary resuscitation (CPR) and first aid at the employee's request. The Agency shall provide first aid kits for each level of the Agency's facility. The names, work telephone numbers and work locations of all employees trained in CPR techniques and first aid shall be provided to the Union. The Agency, the Union, and the employees will cooperate in ensuring that all first aid kits are maintained. The Agency shall promptly contact outside emergency medical or other appropriate employee services when an emergency occurs which warrants this type of assistance.

Section C:

The Agency agrees to maintain clean, sanitary and stocked restroom facilities for bargaining unit employees.

Section D:

1. The Agency agrees to maintain the work place and its equipment in good condition. Deficiencies in this area shall be discussed and brought to the attention of the appropriate authority, and addressed consistent with the applicable rules and regulations.
2. The Union and the Agency shall make every effort to prevent accidents of any kind. If accidents occur, the prime consideration will be the welfare of the injured employee. As promptly as the situation allows, accidents are to be reported to the supervisor by the injured employee and/or his/her co-workers. The supervisor must report injuries to the Agency's Risk Management Officer. A continuous review of security/safety measures shall be the joint responsibility of Management and the Union.

Section E:

When an employee identifies what she/he believes to be an unsafe or unhealthy working condition, the employee shall notify his/her supervisor, who shall investigate the matter and take prompt and appropriate action. If an unsafe or unhealthy condition is determined to exist by the supervisor, the affected employee(s) may not, on a case-by-case basis, be required to perform duties in the affected area. During this period, the supervisor may require the employee(s) to perform their duties in another work area or to perform other duties outside the affected area.

Section F:

When the Agency is aware of a workplace inspection or investigation which is conducted by an Agency safety representative or by an outside agency, such as Office of Risk Management, O S H A or NIOSH, in response to a complaint by the Union or bargaining unit employee, the Union shall be given the opportunity to participate, to the extent permitted by the investigating agency, and to provide information as to issues of concern to bargaining unit employees. During the course of any such inspection or investigation, any employee may bring to the attention of the inspector any unsafe or unhealthy working condition.

Section G:

Employees shall be protected against penalty or reprisal for reporting any unsafe or unhealthy working condition or practice, assisting in the investigation of such conditions, or for participating in any occupational safety and health program and activities.

Section H:

The Agency shall prepare and post instructions to evacuate the building in case of emergency at all Agency locations where bargaining unit employees are assigned. The Agency shall take appropriate action to ensure that employees are familiar with the proper means of leaving the building during a suspected fire bomb threat or other emergencies that require the evacuation of the premises.

Section I:

Within space limitations, the Agency agrees to provide an employee lunchroom which may be used by employees during their lunch period. If this is not possible, Management shall identify space in which employees may eat lunch.

Section J:

The Agency and the Union mutually recognize the need for protection of employees from assault and intimidation at the work place and will work cooperatively towards that end. The Parties agree that mutual respect between supervisors, employees, and co-workers is integral to the efficient performance of the Agency. Behaviors that contribute to a hostile, humiliating or intimidating work environment, including abusive language or behavior, are unacceptable and will not be tolerated. The Parties agree to work cooperatively to prevent and end this kind of treatment.

Section K: Wellness Program

The Parties agree that the wellness of employees can reduce healthcare cost and improve attendance and work productivity. Utilizing the DCHR Wellness Program, reasonable efforts

will be made by the Agency and the Union to promote wellness habits such as increased physical activity, healthy diets and ongoing mental health activities.

Section L: Traumatic Incidents/Stress Defusing

The parties agree that it is in the best interest of the Agency and the employee to allow employees to defuse after dealing with traumatic incidents associated with the performance of their official duties. Therefore, the parties agree to develop a defusing policy during the parties' labor management cooperation committee.

Section M: Employee Assistance Program

1. In accordance with D.C. Official Code § 1-620.07 (3)(2001), it shall be the policy of the Agency to provide employees that have personal problems that may adversely affect their overall work performance or conduct on the job with the opportunity to participate in the Employee Assistance Program (EAP).
2. The parties acknowledge that early identification, documentation and referral of an employee for help can result in improved performance and employee morale. Though participation in EAP is not mandatory, EAP referrals will be made for employees who are experiencing personal problems including, but not limited to, issues which may adversely affect work performance or conduct on the job:
 - a. Family and marital problems;
 - b. Financial difficulties;
 - c. Emotional or mental illness; and
 - d. Substance abuse problems.

Section N: Self-Referrals

1. If an employee recognizes that he/she needs assistance and wishes to consult with an EAP counselor, the employee will request approval from his/her duty supervisor to meet with an EAP counselor during their tour of duty. Such request will not require in-depth explanation of the problems involved.
2. In cases where an employee is requesting accommodations from the Agency to complete an EAP program, the Agency may request confirmation from the EAP provider of the employee's attendance. The Agency agrees it will make every effort to grant such requests.

Section O: Agency Referrals

This type of referral shall be initiated by a manager when management recognizes that there are serious performance and or attendance problems. The manager shall refer the employee to

the EAP. The employees' record of compliance and participation in the EAP shall be released to the Agency only with the employee's consent.

Section P: Discipline

Participation in the EAP is not a prerequisite to the Agency addressing performance and/or attendance problems nor does it restrict the Agency from taking appropriate disciplinary actions in accordance with the disciplinary article of this Agreement, or any other appropriate administrative action.

ARTICLE 9
PERSONNEL FILES

Section A:

The Official Personnel Files of all employees in the bargaining unit covered by this Agreement shall be maintained by the D.C. Department of Human Resources (DCHR).

Section B:

Employees shall have the right to examine the contents of their Official Personnel Folder, upon request, in accordance with regulations and procedures issued by DCHR and shall have the right to obtain copies of any and all official documents therein, subject to D.C. Official Code § 1-631.05.

Section C:

Upon presentation of written authorization by an employee, the Union representative may examine the employee's personnel file and make copies of materials placed in his/her folder.

Section D:

DCHR shall keep all arrests from the Metropolitan Police Department, fingerprint records and other confidential reports in a confidential file apart from the official personnel folder. No person shall have access to the confidential file without authorization from the Director of DCHR.

Section E:

Each employee shall have the right to present any and all information immediately germane to any material or information contained in his or her Official Personnel record. The individual's answer/response shall be attached to the material to which it relates, subject to D.C. Code §1-631.05.

Section F:

Information other than a record of official personnel action is untimely if it concerns an event more than three (3) years in the past upon which an action adverse to an employee may be based. Immaterial, irrelevant, or untimely information shall be removed from the official record upon the finding by the agency head that the information is of such a nature. Prior to the removal of any information in the file, the employer shall notify the employee and give him or her an opportunity to be heard, in accordance with D.C. Code § 1-631.05.

Section G:

The employee shall receive a copy of all material that could result in disciplinary action or may adversely affect the employee, in his/her folder in accordance with present personnel practices. Consistent with the Article, when the Agency places documents in an employee's personnel folder, the employee shall be asked to acknowledge receipt of the document. The employee's signature does not imply agreement with the material but simply indicates he/she received a copy.

Section H:

If an employee alleges that he/she was not asked to acknowledge receipt of materials placed in his/her personnel folder as provided in Section G, the employee will be given the opportunity to respond to the document and the response will be included in the folder.

Section I:

The rights of employees pertaining to their official personnel files shall be extended to apply to any employee personnel files maintained by the Agency.

ARTICLE 10
DISTRIBUTION OF AGREEMENT AND ORIENTATION OF EMPLOYEES

Section A:

When the Agency conducts orientation sessions for new or rehired employees, no more than sixty (60) minutes shall be allocated to the Union to make a presentation and distribute the Union's membership packet. The Agency and the Union shall make available electronic copies of this Agreement to management officials and bargaining unit employees respectively. The Agency will provide the union with one-week advance notice, prior to a scheduled orientation, of an employee's appointment or reappointment.

Section B:

If the Agency fails to conduct an orientation, within thirty (30) calendar days of the employee's appointment or reappointment, the Agency shall allow the Union to conduct an orientation as outlined in Section A of this Article.

ARTICLE 11
PROBATIONARY EMPLOYEES

Employees serving a probationary period shall be entitled to all rights and privileges by virtue of this agreement, excluding, appealing or grieving terminations in accordance with the provisions of the District Personnel Manual.

ARTICLE 12
REORGANIZATION

Section A:

Prior to the Agency's implementation of a reorganization, the agency shall notify the Union, in writing, thirty (30) calendar days in advance of such implementation. Upon request, the Agency shall engage in impact and effect bargaining with the Union.

Section B:

The Agency shall inform the Union upon implementation of any realignment and provide details as to any changes in the internal structure or functions of the Agency as a result of the realignment.

1. **Realignment** - An action which affects the internal structure or functions of an agency, but which does not constitute reorganization.
2. **Reorganization** - The action taken for the purposes of carrying out the objectives of Section 2 of the Governmental Reorganization Procedures Act of 1981, effective October 17, 1981 (D.C. Law 4-42; D.C. Official Code § 1-315.01 (2006 Repl.)), which results in the transfer, consolidation, abolishment, addition, or authorization with respect to functions and hierarchy, between or among agencies, and which affects the structure or structures thereof, and which is subject to adoption by legislative action, including consideration by the Council of the District of Columbia, in accordance with the Act; including but not limited to the: (1) transfer of the whole or part of an agency, or the whole or part of the functions thereof, to the jurisdiction and control of another agency; (2) consolidation of the whole or part of an agency, or the whole or part of the functions thereof, with the whole or part of another agency or the functions thereof; (3) the abolishment of the whole or part of an agency wherein such agency or part thereof does not have or will not have any functions; or (4) authorization of an officer or agency head to delegate functions vested in specific officers or agency heads not presently

authorized to be delegated, except as provided in D.C. Official Code § 1-204.22(6) (2006 Repl. & 2011 Supp.)).

ARTICLE 13
GOVERNING LAWS AND REGULATIONS

Section A:

In the event any D.C. Government-wide or Agency rules, regulations, or policies are in conflict with the provisions of this Agreement, this Agreement shall prevail.

Section B:

If during the life of this Agreement a law or an interpretation of a law by an adjudicatory or administrative body invalidates or requires an amendment to any part of this Agreement, the Parties shall meet promptly upon request of either Party to negotiate the change.

ARTICLE 14
EMPLOYEE RIGHTS

Section A:

All persons shall be treated fairly, equitably, and respectfully in accordance with laws, rules and regulations.

Section B:

All employees shall conduct themselves in a professional and businesslike manner, characterized by mutual courtesy, in their day-to-day working relationships.

Section C:

Any discussions with employees concerning counseling, evaluations, workload reviews, or disciplinary actions will be conducted so as to ensure the privacy of employees. Instructions and guidance shall be given in a reasonable and constructive manner and in an atmosphere that will avoid unnecessary embarrassment before other employees or the public.

Section D:

The Agency and the Union agree that employees have the right to form, join, and assist a labor organization or to refrain from joining, organizing, or affiliating with the Union. Employees shall

not be retaliated against for the exercise of his or her rights under this Agreement, or applicable law.

Section E:

Employees shall be free from interference, restraint, coercion and discrimination in the exercise of their right to organize and designate representatives of their own choosing for the purpose of collective bargaining and labor-management cooperation.

ARTICLE 15
BULLETIN BOARDS

The agency agrees to provide a reasonable amount of space on existing or new bulletin boards and in areas commonly used by employees, in reasonable locations. The Union shall use this space for the purpose of advising members of meetings and any other legitimate Union information.

ARTICLE 16
UNION REPRESENTATIONS

Section A:

One (1) Chief Steward and Two (2) Shop Stewards shall be designated by the Union (Local R3-8) and shall be accorded recognition by the Homeland Security and Emergency Management Agency as representatives for employees in the bargaining unit.

Section B:

The Union will furnish the Agency a written list of elected officials and shop stewards authorized to represent employees. NAGE will submit changes to the Agency as they occur. Recognition will be given only to those representatives whose names have been submitted to the Agency for the purpose of official time.

Section C:

Stewards and elected officials are authorized to perform and discharge the duties and responsibilities of their position as it relates to representing the employees of the Unit.

Section D:

Union representatives who are agency employees shall be permitted official time to engage in the following labor-management activities:

1. Investigation, receipt, preparation and presentation of grievances and safety issues;
2. Labor-Management and safety committee meetings;
3. Preparation and presentation in arbitration, PERB, OEA, OHR, and other applicable jurisdictional bodies;
4. Attending meetings with Agency, Mayor, City Council, Congress or official body;
5. Attending negotiation meetings as designated member of team or acting as alternate for absent member;
6. Consulting with Agency or its representatives, other Union representative, or employees, concerning enforcement of Agreement;
7. To attend training or other activities to further the interests of improving the Labor-Management relationship; and
8. Travel to any of the activities listed above.

Section E:

The term "Official Time" as used in this agreement shall mean an approved absence from duty by a recognized union official during regular hours of duty without loss of regular or premium pay and without charge to annual leave, sick leave or compensatory time, for official union business.

Section F:

Request for official union time will be made in advance on the Official Time Form. Official time must be requested and approved through the division manager or designee. Designated representatives will request release from their division manager or designee. The Union agrees to comply with all leave requirements as outlined in this agreement when official time is not being used.

Section G:

1. Requests by Stewards to meet with employees or requests of employees to meet with Stewards shall not require prior explanation to the division manager of the problems involved other than to identify the area to be visited, and the general nature of the Union business to be conducted.
2. The Union and employees recognize that workload and scheduling considerations will not always allow for the immediate release of employees from their assignments. The Division Manager may deny access based on workload or staffing reasons, but will

provide access at the earliest feasible opportunity. The Agency agrees that, while discretion for release lies with the employee's Division Manager, such permission for release shall not be unreasonably delayed.

Section H:

A Union representative, when leaving work to transact permissible official union business as defined by this Agreement during work hours, first shall request permission and receive approval from his/her Division Manager. If no reply is received from the Union's representative's division manager, the request for official time shall be deemed approved. The employee must submit the attached "Official Time Form" each pay period to memorialize the use of approved official time for time and attendance accounting.

Section I:

1. Upon entering a work area other than his/her own, the Union representative shall advise the appropriate division manager of his/her presence and the name of the employee he/she desires to visit. In the event the Union representative wishes to visit a work area but not to meet with a bargaining unit member, he/she must notify the appropriate division manager upon arrival.
2. Non-employee union representatives must give one (1) hour of advance notice prior to entry into any Agency facility to conduct union business. Said notice must be provided to the Agency Labor Liaison or his/her designee.

Section J:

1. A one year trial period will be established to quantify the amount of official time that will be granted by HSEMA to NAGE to conduct official union business during work hours. During this trial period, the Agency agrees to provide the Union with 416 hours of official time annually to be used in the calendar year for the purpose of conducting union representational duties that are directly related to HSEMA bargaining unit members' terms and working conditions. The hours may be distributed by the Union President as deemed necessary. If it becomes necessary during this trial period for the use of more than the 416 official time hours, additional official time may be granted on a case-by-case basis. Reasonable request for official time beyond the 416 hours will not be unreasonably denied. During this trial period, labor management, safety committee meetings or meeting requests initiated by management will not count against official time hours.
2. Upon conclusion of the trial period, the Agency and the Union agree that the undisputed number of official time hours used during the trial period will be the annual allotment for the duration of the contract.

Section K:

The Union may select five (5) employees from the list of written elected officials and shop stewards who will each receive up to 40 hours of official time annually for the purpose of training to enhance labor management relations. The Union will provide 14 days' notice when requesting such leave. The Agency will respond to this request within seven (7) days.

Section L:

The Union agrees that grievances should preferably be investigated, received, processed and presented at a time when Agency performance standards will not be compromised unless otherwise authorized. The Agency will not prevent Union representatives from representing employees at reasonable times consistent with the provisions of this Agreement.

Section M:

The Agency shall make every reasonable effort to notify the Union and the steward no later than 14 working days prior to placing Union representatives on details or making shift changes. In no case shall such action be taken as a means of retaliation.

ARTICLE 17
UNION SECURITY AND UNION DUES DEDUCTIONS

Section A:

The terms and conditions of employment contained in this Agreement shall apply to all bargaining unit employees without regard to Union membership. Employees covered by this Agreement have the right to join or to refrain from joining the Union.

Section B:

1. Pursuant to D.C. Official Code §1-617.07 (2001 Edition), the Employer shall deduct dues from the bi-weekly salaries of those employees who authorize the deduction of said dues. The dues check-off authorization may be cancelled by the employee at any time upon written notification to the Union and the Employer. When Union dues are cancelled, the Employer shall withhold a service fee without written authorization.
2. The employee's authorization (D.C. Form 277) shall be forwarded to the Office of Labor Relations and Collective Bargaining (OLRCB).

Section C:

Each employee's Union dues and service fees shall be transmitted to the Union, minus \$0.10 to the OLRCB for the administrative costs associated with the collection of said dues and service fees.

Section D:

Payment of dues or service fees shall not be a condition of employment.

Section E:

1. The service fees for bargaining unit employees who are not members of the union shall be equal to the proportionate share of the union's costs of negotiating and administering the collective bargaining agreement and adjusting the grievances and disputes of bargaining unit employees.
2. The union shall be solely responsible to providing notice of the service fee to bargaining unit employees who are not members.
3. The Union shall notify the Employer of the pro-rata amount to be paid for service fees should it result in a change in service fees payable by any unit member. The Union shall adhere to all applicable laws in this regard.

Section F:

The Union shall indemnify, defend and otherwise hold the employer harmless against any and all claims, demands and other forms of liability, which may arise from the operation of this Article. In any case in which a judgment is entered against the employer as a result of the deduction of dues or other fees, the amount held to be improperly deducted from an employee's pay and actually transferred to the Union by the Employer, shall be returned to the Employer or conveyed by the Union to the employee(s), as appropriate.

ARTICLE 18
CONTRACTING OUT

It is recognized that contracting out of work that is normally performed by employees covered by this Agreement is of mutual concern to the Agency and the Union. When there will be adverse impact to bargaining unit employees, the Employer shall meet with the Union within 60 days prior to final action, except in emergencies. The Union shall have full opportunity to make its recommendations known to the Employer who will duly consider the Union's position and give reasons in writing to the Union for any contracting out action. The Agency agrees to abide by appropriate District regulations regarding contracting out.

ARTICLE 19
VACANCY ANNOUNCEMENTS

Section A:

All vacancy announcements for positions covered by this Agreement shall be distributed via email and posted on all bulletin boards within the Agency for a minimum of ten (10) calendar days and posted on the District's web site.

Section B:

Employees must submit an application in the manner outlined in the announcement to be considered. The Agency will notify all unsuccessful candidates in the bargaining unit of their non-selection within 30 working days, by email, after the selection has been made.

Section C:

Where all other factors are equal among qualified applicants, the vacancy shall be filled by the qualified applicant who has seniority in the Agency.

Section D:

Employees may individually or with a Union representative request a final review of a specific promotion action for which they applied and were not selected.

Section E:

The Union president or designee shall be provided with a copy of all vacancy announcements in the Agency by email.

ARTICLE 20
REDUCTION IN FORCE

Section A:

The Agency agrees that reductions-in force will be conducted in accordance with the procedures set forth in D.C. Official Code § 1-624.02.

Section B:

The Parties agree that an employee identified for separation from his or her position through a reduction-in-force action may appeal his or her separation only in accordance with D.C. Official Code § 1-624.08. A reduction-in-force action is not a grievable matter under this Agreement.

Section C:

In the event of a reduction-in-force, the Agency shall engage in impact and effect bargaining, upon request by the Union.

Section D:

When requested by the Union, the Agency agrees to provide the Union with information that is relevant and necessary for the Union to engage in impact and effect bargaining.

ARTICLE 21
SCHEDULING/ HOURS OF WORK

Section A:

Except when the HSEMA director determines that activation is necessary, the working hours in each day in the basic workweek shall be the same.

Section B:

1. Work schedules showing the employees shift, work days and hours shall be posted and made known to the employee.
2. Work schedules shall be established for employees who are assigned in a twenty-four hour operational unit and are required to work on Saturday and/or Sunday as part of their regular workweek. These schedules will be followed when scheduling bargaining unit employees to their various tours of duty, which shall be consistent with DC law. Work schedules for employees assigned to these units shall be made known to the employee.

Section C - Changes in Work Schedule:

Prior to any changes to the employee's work schedule, the employer shall provide the employee with a 14 day written notice, absent emergencies or activation. The employer will also furnish the employee with the reason(s) for the change in the work schedule.

Section D:

An employee's schedule shall not be changed for brief periods of time or on short notice for the sole purpose of avoiding the payment of overtime.

Section E:

When an employee is required to attend a mandatory training, off duty, he/she shall be compensated. The compensation may consist of overtime, compensatory time or an additional day off. However, prior to the training, the employee and his/her supervisor shall determine the compensation the employee will receive.

Section F - Rest Periods:

1. Employees will be provided a break every 4 hours, one of which will be an unpaid 30 minute lunch break.
2. Employees will be provided with one additional 15 minute break for every (2) hours worked beyond the regular tour of duty. The same principle shall apply for overtime.

ARTICLE 22
ADMINISTRATION OF
LEAVE

Section A - General:

In an effort to provide the Union with an opportunity to counsel employees with attendance issues prior to the issuance of a leave restriction letter or letter of warning, the employer shall provide as applicable to the Union President or his or her designee with a list of employees suspected of abusing sick leave, employees with excessive or unscheduled emergencies or employees who are continually late for duty. The Union President shall provide the Agency a current list of authorized representatives to participate in this activity. Upon receipt of the list, the union official and/or steward shall counsel those employees in an effort to educate them regarding attendance problems and or issues. This procedure will not prevent corrective or adverse action when deemed necessary by the Agency.

Section B - Annual Leave:

1. Employees may submit leave at any time during the calendar year.
2. The employee shall request annual leave from the division manager or designee. Agency agrees to provide the employee an opportunity to use the annual leave that is earned. Requests for annual leave will not be denied without sufficient cause. Leave previously approved will not be cancelled or rescheduled by the Agency without a good and sufficient reason, which shall be in writing in the remarks section on the DCSF-71.
3. Any normal requests for accumulated annual leave must be submitted on a DCSF-71 to the division manager or designee. Requests for three (3) days or less shall be

requested at least two (2) days in advance. Requests for annual leave in excess of four (4) days or more shall be submitted at least four (4) days in advance. The duty supervisor or designee shall respond to the employee leave requests no later than twenty-four (24) hours after receipt of the request for leave or the end of the employees next working day.

4. An alternative or compressed work schedule shall not affect the existing leave system. Leave will continue to be earned at the same number of hours per pay period as the employees on five (5) day, forty (40) hour schedules and will be charged on an hour-by-hour basis.
5. It is the responsibility of the employee to notify his/her supervisor of the need for emergency leave prior to the start of his/her tour of duty. Call in for emergency annual leave shall be at the earliest practical time, in no event less than one hour prior to the start of the shift; and will state the reason for the requested leave and the expected duration. In the event of an unforeseen emergency, a family member may contact the employee's supervisor; however, the employee must make direct contact with his/her supervisor or the next higher level manager as soon as practical but no later than the end of the employee's tour of duty. Every effort will be made to make direct contact with the supervisor prior to the end of the employee's tour of duty.
6. Requests for annual leave shall be approved on a first received basis. But in the event two or more requests for the same period are received on the same day and staffing requirements prevent the granting of all such requests, the conflict shall be resolved on the basis of employee seniority as determined by service computation data.
7. Employees shall receive a lump sum payment for all annual leave not used at retirement, resignation or separation in accordance with District Personnel Manual.
8. The Agency staffing needs shall be considered when approving leave. All requests for annual leave shall be approved in a fair and equitable manner.

Section C - Sick Leave:

1. Accrued sick leave shall be granted to employees incapacitated by illness and unable to perform their duties. Sick leave may also be used by employees to care for immediate family members in accordance with D.C. Official Code § 32-501. Immediate family members will be recognized as defined in D.C. Official Code § 32-701 (2001 Ed.). Employees shall request sick leave as soon as possible on the first day of sickness.
2. To the extent possible, sick leave shall be requested and approved in advance for visits to and/or appointments with doctors, dentists, practitioners, opticians, chiropractors, etc. and for the purpose of securing diagnostic examinations, treatments and x-rays.

3. Employees shall not be required to furnish a doctor's certificate to substantiate requests for approval of sick leave unless such sick leave exceeds three (3) workdays of continuous duration or the employee is on sick leave restriction. However employees may submit medical certificates for sick leave occurrences that are less than three (3) days in duration, management will accept such slip and properly document the submission of a medical certificate for the occurrence.
4. In cases of serious disability or ailment, advance sick leave may be granted to permanent employees in amounts not to exceed 240 hours.
 - a. The request must be in writing and must be supported by an acceptable medical certificate.
 - b. All available accrued and accumulate sick leave must be exhausted. The employee must use annual leave he/she might otherwise forfeit.
 - c. The request should be denied only if the requirements of (a) and (b) are not met or there is reason to believe that the employee will not return to duty or may not be able to repay the advanced leave.

Section D - Maternity Leave:

Maternity leave shall be granted to pregnant employees upon request. Maternity leave may be any combination of accumulated leave and leave without pay. Employees requesting maternity leave should provide reasonable advance notice to their supervisors and state how much leave they are requesting.

Section E - Paternity Leave:

Paternity leave, including for a legal guardian, shall be granted for a period of up to two (2) weeks following the birth of a child (natural, adopted and foster child). An employee requesting Paternity Leave shall be given priority consideration over the provisions as contained in Section B -Annual Leave.

Section F - Family and Medical Leave:

The agency shall grant employees FMLA leave in accordance with D.C. Official Code § 32-501 et seq. (2006). Employees are entitled to apply for both D.C. FMLA and federal FMLA as outlined in the applicable rules and regulations thereof.

Section G - Leave without Pay:

An employee may be granted leave without pay, up to one (1) year, in the event of serious illness and upon expiration of accumulated sick leave in accordance with the provisions of the District of Columbia Personnel Manual (DPM), Chapter 12, Part II, Subpart 5.

Section H - Leave for Donating Blood :

Employees shall be granted paid leave not to exceed four (4) hours on any one occasion per year for the purpose of donating blood.

Section I - Court Leave:

Employees shall be granted leave of absence with pay anytime they are required to report for jury duty or to appear as a witness on behalf of the District of Columbia government, or Federal or a State or Local Government. A night-shift employee who performs jury or witness service during the day shall be granted court leave for his or her regularly scheduled night tour of duty.

Section J - Funeral Leave:

Bereavement leave shall be granted in accordance with the Compensation Units I & 2 Agreement.

Section K: SWAP:

For the purposes of this agreement a SWAP is defined as: A voluntary exchange of tours of duty between employee(s) with like qualifications and/or skill set. Request for a swap must be submitted to the employee(s) division manager or designee on the designated swap form. Such request must be submitted at least one (1) week in advance and must take place within the same work week. SWAPS must not result in a negative impact on the agency.

ARTICLE 23
DISCIPLINE

Employees shall be disciplined for cause in accordance with Chapter 16 of the District Personnel Manual. Discipline shall be administered in a fair and equitable manner, so as not to create an unreasonable delay. Discipline shall be appropriate to the circumstances and shall be corrective rather than punitive in nature, and shall reflect the severity of the infraction.

Section A:

1. Employees have the right to advance notice where appropriate, and an opportunity to respond to proposed discipline pursuant to the provisions of Chapter 16 of the DPM.
 - a. **Admonition** – any written communication from a supervisor or manager to an employee up to but excluding, an official reprimand, that advises or counsels the employee about conduct or performance deficiencies, and the possibility that future violations will result in corrective or adverse action.

- b. A corrective action shall be an official reprimand, or suspension of less than ten (10) days.
- c. An adverse action shall be a suspension of ten (10) days or more, a reduction in grade, or removal.
 - i. In the case of a proposed corrective action, employees shall receive an advance written notice of ten (10) days.
 - ii. In the case of a proposed adverse action, employees shall receive an advance written notice of fifteen (15) days.
- 2. The Agency shall take action only in accordance with the progressive discipline table of offenses as contained in the Table of Penalty Guide as approved by the District of Columbia Department of Human Resources.

Section B:

- 1. Employees have the right to contest adverse actions through either the Office of Employee Appeals (OEA) or the negotiated grievance procedures. Corrective actions may only be contested through the grievance procedure. An employee is deemed to have elected his or her forum at the time of filing. Once the employee has selected the forum, the selection cannot be changed.
- 2. Should the employee elect to appeal the action to OEA, such appeal shall be filed in accordance with OEA regulations.
- 3. Should the employee elect to grieve under the negotiated grievance procedure, the grievance must be filed pursuant to the Grievance and Arbitration article of this contract.

Section C:

- 1. An employee or the employee's representative shall be provided up to four (4) hours of administrative leave to prepare for his/her response to a proposed corrective action, and up to eight (8) hours of administrative leave to prepare for his/her response to a proposed adverse action.
- 2. If the Agency has reason to counsel an employee, it shall be done so as not to unnecessarily embarrass the employee before other employees or the public.
- 3. At any investigatory interview which the employee reasonably believes may result in discipline, an employee may request to have a Union representative present at said meeting. Such requests shall not be denied.

Section D:

The Agency should consider, in appropriate cases, referring to EAP employees who are experiencing problems that adversely affect their overall work performance, and whether referral is warranted to assist the employee in improving his or her work performance and/or attendance. Participation in the EAP is not a prerequisite to the Agency addressing performance and/or attendance problems nor does it restrict the Agency from taking appropriate disciplinary actions in accordance with the disciplinary article of this Agreement, or any other appropriate administrative action.

ARTICLE 24
GRIEVANCE/ARBITRATION PROCEDURES

Section A:

1. The purpose of this Article is to provide a mutually acceptable method for the prompt and equitable settlement of grievances.
2. Therefore, the Agency and the Union retain the right to settle any grievance in the enforcement of *this* Agreement through and including Step 4 of the grievance process. The Agency shall ensure that all settlements reached with respect to grievance resolution shall be implemented.

Section B:

A grievance is a complaint by any *unit* employee, the Union or Agency that there has been a violation, misapplication or misinterpretation of:

1. This agreement
2. A violation or misapplication of appropriate term(s) and condition(s) of the Compensation Agreement for Units 1 & 2.

Section C - Presentation of Grievance:

This procedure is designed to enable the parties to settle grievances at the lowest possible administrative level.

Categories of Grievances:

1. Personal: A grievance of a personal nature requires signature of the aggrieved employee at Step 1 even if the grievant is represented by the Union.
2. Group: If a grievance involves a group of bargaining unit employees within the Agency, the grievance may be filed by the Union on behalf of the group of employees at the appropriate step of the grievance procedure where resolution is possible. When filed by the Union, the grievance must be signed by the Union President or his or her designee. Such designation must be in writing and signed by the President. A group grievance must contain all information specified in Step 1 of the grievance procedure and be signed by each member of the group.
3. Class: A grievance involving all the employees in the bargaining unit must be in writing and filed and signed by the Union President or his or her designee; such designation must be in writing and signed by the President. Grievances so filed will be processed only if the issue raised is common to all unit employees. A class grievance must contain all information specified in Step 1 of the grievance procedure.

Section D:

In the event that an individual grievant, group or class is not represented by the Union, the Union shall be given the opportunity, pursuant to advance notification, to be present and offer its view at any meeting held to adjust the grievance. A copy of any settlement agreement reached between the parties or adjustment, decision or response made by the Agency must be sent to the Union.

Section E- Procedure:

The Parties agree that in the event of the emergency operating center of National Special Security Event (NSSE) designated by the Department of Homeland Security activation, the timelines set forth in the section E, Steps one (1) through four (4) will be suspended during the time of the activation.

Step 1:

The aggrieved employee and, should the employee so elect, a Union representative, shall present the grievance in writing to the division manager, or designee within ten (10) business days of the occurrence of the event giving rise to the grievance, or within ten (10) business days of the employee's or Union's knowledge of such event. The division manager, or designee shall make a decision on the grievance and reply to the employee and his/her

representative within ten (10) business days after written presentation of the grievance. The grievance at this and subsequent steps shall contain:

- a. Description of the nature of the grievance;
- b. The date(s) on which the alleged violation occurred;
- c. A complete citation to provisions allegedly at issue
- d. A statement of the remedy or adjustment sought; and
- e. The signature of the aggrieved employee(s) and the Union representative, if applicable, according to the category of the grievance.

Step 2:

If the grievance is not settled, the employee with or without his/her Union representative, shall submit a signed, written grievance to the Agency Labor Liaison within ten (10) business days following the Division Manager's written response or the date said response was due.

The Agency Labor Liaison shall submit a signed, written response to the employee or his/her representative within (10) business days of its receipt.

Step 3:

If the grievance remains unsettled, the grievance shall be submitted to the Agency Director or his or her designee within 15 business days following receipt of the Step 2 response or the date said response was due. Within 15 business days of the Step 2 grievance the Director or his/her designee may meet with the aggrieved employee and his/her representative to attempt to resolve the grievance or respond in writing. When the meeting occurs, the Director shall respond in writing to the employee and his/her representative within 15 business days following the Step 3 meeting.

Step 4:

If the grievance remains unsettled, the Union within 15 business days from receipt of the Director's response, shall advise the Office of Labor Relations and Collective Bargaining (OLRCB) in a signed statement should the Union intend to request arbitration of the matter on behalf of the employee(s). Only the Office of Labor Relations and Collective Bargaining or the Union can refer a grievance to arbitration. If the Union does not demand arbitration within 15 business days of the receipt of the Director's decision, the Director's decision is final and binding.

Section F:

Should the grievance, at any time, not contain the required information, the grievant shall be so notified in writing and given five (5) working days from receipt of notification to resubmit the grievance.

Section G:

If the agency fails to provide a response as outlined in the aforementioned steps of the grievance procedures, the union or employee may proceed to the next step of the grievance process, and take the failure to provide a response as a denial of the grievance.

Section H - Grievance Mediation:

The purpose of this Grievance Mediation procedure is to provide, a method by which the parties may mutually reach satisfactory solutions to grievances prior to the invocation of arbitration. The parties recognize the necessity of carefully considering the circumstances of the particular grievances in deciding whether to utilize this procedure. This procedure, while broadening the channels of grievance resolution, must comply with District of Columbia laws, rules, regulations and the negotiated grievance procedure and shall only be invoked upon mutual agreement of the parties in writing on a case-by-case basis.

1. Selection-Should the parties fail to resolve the grievance utilizing the grievance procedure set forth above (Section G), the parties may, within ten (10) workdays after the Union's request for arbitration pursuant to Step 4 of the grievance procedure, mutually agree to utilize the mediation process as set forth below.
 - a. A joint request shall be submitted to the Federal Mediation and Conciliation Services (FMCS) or other appropriate authority that provides grievance mediation services, with which the parties jointly agree. The mediator selected must have demonstrated expertise in public sector labor relations and in grievance mediation.
 - b. The mediation session(s) must commence within thirty (30) days of the Agreement to mediate and must conclude prior to the date scheduled for the start of the arbitration requested pursuant to the procedures established in Section D of this Article.
2. Mediation Procedure:
 - a. Each party shall have representation at the mediation session.

- b. The grievant(s) shall be present and participate at the mediation session. In the case of a class or group grievance, a maximum of three (3) of the aggrieved of a class or group grievance shall be present as representatives of the class or group.
- c. Mediation sessions shall be informal. The rules of evidence shall not apply.
- d. The mediation session shall be confidential. No record of the session shall be made.
- e. During the session, the mediator may meet individually or jointly with participants, however, he/she is not authorized to compel or impose a settlement.
- f. The mediation session shall not exceed one (1) day unless the parties agree otherwise.

3. Mediation Conclusion:

- a. The parties shall sign their respective copies of any Settlement Agreement as a result of mediation.
- b. Should both parties accept the settlement, it shall not have precedent- setting value unless mutually agreed to on a case-by-case basis. Absent mutual agreement neither party may cite any settlement achieved through mediation in any other proceeding.

Section I - Arbitration:

The parties agree that arbitration is the method of resolving grievances which have not been satisfactorily resolved pursuant to the grievance procedure and may be used by the Union to appeal disciplinary actions.

Section J:

Within 30 days of the decision of the Agency Director on a disciplinary action as the final Agency Action, the Union, on behalf of an employee, may advance the matter to arbitration.

Section K: Selection of an Arbitrator:

Except in cases of mutual agreement as to the appointment of an arbitrator, the party demanding the appointment of an arbitrator may file with either the American Arbitration Association (AAA) or the Federal Mediation and Conciliation Services (FMCS). The AAA or FMCS shall be requested by the party demanding arbitration to provide a list of at least seven (7) arbitrators from the sub-regional Washington, D.C. metropolitan area from which an arbitrator shall be selected after receipt of the list by both parties. When either party requests a panel, the FMCS or AAA shall be provided with the name and address of the Office of Labor Relations and Collective Bargaining as the representative of the Employer. The Party requesting the

panel shall bear the fees associated with the panel request and any initial administrative fees. Both the Employer and the Union may strike three (3) names from the *list* using the alternate strike method. The party requesting arbitration shall strike the first name.

Section L:

If, before the selection process begins, either party maintains that the panel of arbitrators is unacceptable, a request for a new panel from AAA or FMCS shall be made. Subsequent requests can be made until the parties receive an acceptable panel.

1. Either party may dispute that a valid collective bargaining agreement exists between the parties or that the substantive matter in dispute is not within the scope of the collective bargaining agreement.
 - a. The Parties agree that under the current law in the District of Columbia, the substantive issue of whether a particular subject matter is subject to arbitration under the parties CBA is an issue for judicial determination. The threshold issue of arbitrability is within the exclusive jurisdiction of the District of Columbia Superior Court. *See, Washington Teachers' Union Local #6, et al v. District of Columbia Public Schools*, 77 A.3d 441 (D.C. 2013). If legislation is passed changing the law or *Washington Teachers' Union* is overturned by the court, the Parties agree to immediately re-visit and re-negotiate this provision in order to determine the appropriate process for establishing arbitrability under this agreement. Disputes regarding whether a matter is or is not substantively arbitrable under the Parties' CBA will be decided under the rules outlined in D.C. Official Code §16-4407.
 - b. If a Party asserts a matter is not substantively arbitrable and a Party files to compel or stay arbitration under the D.C. Official Code § 16-4407, the unsuccessful Party at Superior Court shall pay the filing costs/fees for filing in superior court of the successful Party.
2. Hearings shall be held in the Office of Labor Relations and Collective Bargaining Negotiation Center or another mutually agreeable location. If any additional costs are involved, they shall be borne equally by the parties.
3. The arbitrator shall hear and decide only one (1) grievance in each case unless the parties mutually agree to consolidate grievances.

4. The arbitration hearing shall be informal and the rules of evidence shall not strictly apply.
5. The hearing shall not be open to the public or persons not immediately involved.
6. Witnesses shall be sequestered upon request of either party.
7. Either party to the arbitration has the right to have a verbatim stenographic record made at its own expense. The expense may be shared upon mutual agreement in advance of the hearing. The stenographic company shall provide the Arbitrator a copy of the record. Stenographic records are not producible pursuant to a request by either party unless that party has paid for all or part of the cost of said record pursuant to a mutual agreement. If the Union intends to share the cost of the record of the hearing it must notify the Office of Labor Relations and Collective Bargaining at the time of scheduling the hearing.
8. The parties shall attempt to submit a written joint statement of the issue or issues to the arbitrator, and if not, shall each submit separate statements.
9. The parties shall exchange witness lists in writing five (5) days prior to the date the hearing is commenced. District employees will be on-call and will be released to testify as requested by either party.
10. The arbitrator's award shall be in writing and shall set forth the arbitrator's findings, reasoning and conclusions within thirty (30) days after the conclusion of the hearing or within thirty (30) days after the arbitrator receives the briefs, if filed, whichever is later.
11. The arbitrator shall not have the power to add to, subtract from, or modify the provisions of this Agreement through the award. The arbitrator shall confine his/her award to the issue(s) presented. The Arbitrator's award shall not conflict with any provision of applicable law. The arbitrator shall not retain jurisdiction of the case once his or her decision is issued.
12. The arbitrator shall have full authority to award appropriate remedies consistent with law.
13. The arbitrator's award shall be binding upon both parties.
14. A statement of the arbitrator's fee and expenses shall accompany the award. The fees and expenses of the arbitrator shall be borne equally by the parties.

Either party may appeal the arbitrator's award in accordance with applicable law and regulations.

Section M: General:

1. All time limits shall be strictly observed unless the parties mutually agree to extend said time limits.
2. The presentation and discussion of grievances shall be conducted at a time and place which will afford a fair and reasonable opportunity for both parties and their witnesses to attend. Such witness(s) shall be present only for the time necessary for them to present evidence. When discussions and hearings required under this procedure are held during the work hours of the participants, all unit employees required to be present shall be excused with pay for that purpose.
3. If either party considers a grievance to be either substantively or procedurally non-grievable or non-arbitral, that party shall so notify the other party prior to the date of the hearing.
4. A party does not waive its rights to present procedural defenses by failing to raise the issue before the start of the arbitration hearing.

ARTICLE 25
DISTRICT PERSONNEL MANUAL

The Agency shall make available to the Union any portion of the D.C. Personnel Manual that is not available on the District's web site. The Agency shall furnish the Union with a copy of all Agency regulations.

ARTICLE 26
FACILITIES AND SERVICES

The Agency agrees to the use of its facilities for meeting purposes for the union subject to the following conditions:

1. The use of facilities will not involve any additional expense to the District Government other than the normal expenses which are incurred for items such as heating and lighting.
2. The Union will request in writing the use of D.C. Government facilities for the purpose of Union meetings no later than five (5) working days in advance of requested meeting date. The Agency will reply within two (2) working days of initial request.

3. The Union recognizes its responsibility in using District facilities to observe all applicable security and public safety regulations and to conduct its meetings in an orderly manner so as not to interfere with normal work operations, and assumes responsibility for all damages to District property occasioned by their use, and agrees to leave the facility in a clean and neat condition.
4. The employer agrees to provide the union with an office of a size to accommodate a desk, one (1) computer with access to a printer, two (2) chairs, a file cabinet, a telephone, for the purpose of conducting union business. The office will lock.

ARTICLE 27

DETAILS AND TEMPORARY PROMOTIONS

Section A:

A detail is the temporary official assignment of an employee to a different position or duties.

Section B:

1. An employee may be detailed to another position to meet a temporary employment need for a period of not more than 120 days to an unestablished position or 240 days to an established position.
2. Employees detailed to perform the duties of a higher graded position for 60 or more consecutive days, shall receive the pay of the higher graded position, effective the first pay period which begins on or after the 61st day.
3. The applicable rate of pay will be determined by application of D.C. Government procedures concerning grade and step placement for temporary promotions.
4. An employee on detail to a lower graded position shall maintain the pay for his/her original position.

Section C:

This provision shall not apply to training programs.

Section D:

Details shall not be made as a means of retaliation.

ARTICLE 28
SAVINGS CLAUSE

Section A:

1. In the event any article, section or portion of the Agreement should be held invalid and unenforceable by any Court or higher authority of competent jurisdiction, such decision shall apply only to the specified Article, Section or portion thereof specified in the decision; and upon issuance of such a decision, the Employer and the Union agree to immediately negotiate a substitute for the invalidated Article, Section, or portion thereof.
2. This collective bargaining agreement represents the complete agreement between the Parties for the term and cancels and supersedes any and all previous agreements entered into between the Parties.

ARTICLE 29
CAREER LADDER

Section A:

Career ladder is defined as a series of positions in the same line of work whose duties increase in difficulty from the entrance level to the level established as full performance. Employees may be promoted in it without further competition until reaching the full-performance level. Although initial competition covers the entire career ladder, such promotions are not guaranteed. The following requirements must be met each time such promotion is made:

1. Time in grade;
2. Demonstration to the satisfaction of the supervisor the ability to perform at the next higher level;
3. Meeting appropriate minimum qualifications, including selection criteria; and
4. There shall be a demonstrated need for the higher-level work to be performed.

Section B:

An employee may receive successive career ladder promotions until he/she reaches full performance level in a career ladder series, after meeting the qualifications required for each level

ARTICLE 30
NEW TECHNOLOGY

Section A:

Both parties recognize the exclusive rights of management to acquire and implement new technology. The Parties recognized management's obligation to provide the Union with advance notice, and if requested, the Unions right to engage in impact and effects bargaining.

Section B:

The Agency agrees to provide written notice to the union to include a description of the new technology and the approximate timing for implementation.

Section C:

Prior to implementation of any new technology that has a substantial impact on the terms and working conditions of bargaining unit employees, the Union upon request, shall be provided with the opportunity to engage in impact and effect bargaining. Impact and effect bargaining will not delay the implementation of the new technology.

Section D:

The Agency shall provide appropriate training to all bargaining unit employees impacted by the new technology. If possible, the training shall be conducted during the employees' regular tours of duty. If such training cannot be conducted during the employees' regular tour of duty, the employee shall be compensated in accordance with the Compensation Agreement for Compensation Units 1 & 2.

ARTICLE 31
SENIORITY

Section A:

Seniority is defined by an employee's length of continuous service in a position, for the purposes of this Agreement only. Seniority may be considered in making decisions about shift changes, leave approvals and other working conditions. Seniority determinations shall be made in the following order:

1. Time in position;
2. Employees hired on the same day shall use alphabetical order of surname; and
3. Service computation date.

Section B:

An employee(s)' continuous service shall be broken by voluntary resignation, discharge for cause or retirement. If an employee returns to his former, or comparable, position within one year, the seniority he had at the time of his/her departure will be restored but he/she shall not accrue additional seniority during his/her period of absence.

Section C:

The Agency shall provide the Union annually with a list of names of employees represented by the Union. The list will be in seniority order as defined by this article. The agency shall also provide the Union annually with a list of new hires in bargaining unit positions and with names of unit employees who have left the Agency since the last seniority list.

**ARTICLE 32
ADMINISTRATION OF OVERTIME**

Section A:

Overtime work shall be equally distributed among employees. Individual employee qualifications shall be considered when decisions are made on which employees shall be called for overtime work.

Section B - Anticipated Overtime:

Work that is necessary to be performed on an overtime basis that is known and can reasonably be planned for and scheduled in advance.

1. Anticipated overtime assignments shall be scheduled and posted as far in advance as practical, but no less than 24 hours in advance.
2. Employees working anticipated overtime are responsible for reporting for overtime assignments in accordance with the requirements of a regular tour of duty absent extraordinary circumstances. When such circumstances are encountered, the employee will contact the on-duty supervisor as soon as possible for the purpose of requesting an excusal.

Section C - Unanticipated Overtime:

Is work necessary to be performed on an overtime basis that is not known, or cannot reasonably be planned for and scheduled in advance. This includes, but is not limited to overtime work that cannot be scheduled in advance due to fluctuations or uncertainties in operational requirements.

1. Management shall first solicit volunteers when unanticipated overtime work is required.
2. **On duty employees** – Management will make every effort to notify employees at least one (1) hour or the earliest practical time in advance of the end of their tour of duty in cases of forced overtime. In the event a sufficient number of qualified volunteers are not available to perform the unanticipated overtime, overtime will be assigned as follows:
 - a. Unanticipated – (forced overtime) overtime work will be assigned to equally qualified employees in inverse order of seniority.
 - b. Unanticipated (Volunteers) – Overtime shall first be distributed based on the minimum skill set required of the position.

Section D - Qualified Employee:

Qualified Employee means one that possesses the required knowledge, skills and abilities necessary to perform a particular assignment. Overtime shall first be distributed based on the minimum skill set required of the position.

Section E:

When employees' services on an overtime basis are determined not to be needed prior to the start of the assignment, every attempt will be made to notify the affected employee in sufficient time to prevent the employee from reporting to duty. In the event that an employee is not notified they shall be credited a minimum of two (2) hours of overtime in accordance with the provision of the Compensation Agreement for Compensation Units 1 & 2, if subsequently sent home.

Section F:

Absent operational emergencies, employees will not be scheduled to work a combination of regular and/or overtime assignments that do not allow for eight (8) consecutive hours off-duty within each twenty-four (24) hour period. This twenty-four (24) hour period begins when the employee first reports to work (either on regular time or on an overtime basis) after an off-duty period.

Section G - Overtime Trades:

In order to mitigate potential adverse impact resulting from overtime assigned through involuntary drafts, management will approve employee requests to trade overtime assignments provided the employees involved in the trade are equally qualified to perform the trade assignment and the trade does not result in a negative impact to the agency. A trade is defined as the voluntary exchange of overtime assignments between two employees.

Article 33
TRAINING, LICENSING AND CERTIFICATIONS

Section A:

Training that is required and/or a condition of employment shall be at the expense of the Agency. If possible, the training shall be conducted during the employee's regular tour of duty. If such training cannot be conducted during the employees regular tour of duty; the employee shall be compensated in accordance with the Compensation units 1 and 2 Agreement.

Section B:

When it is determined by the Agency that employees holding certain positions are required to be certified or licensed as a condition of employment, maintaining such certificates or licensing shall be at the expense of the Agency.

ARTICLE 34
DURATION AND FINALITY

Section A:

This Agreement shall remain in full force and effect until September 30, 2017. The Agreement will become effective upon ratification by the Union and the Mayor's approval subject to the provisions of D.C. Official Code §1-617.15 (2001 Ed.). If disapproved because certain provisions are asserted to be contrary to applicable law, or if not ratified by the Union, the Parties shall meet within thirty (30) days to negotiate a legally constituted replacement provision or the offensive provision shall be deleted.

Section B:

1. The Parties acknowledge that this contract represents the complete Agreement arrived at as a result of negotiations during which both parties had the unlimited right and opportunity to make demands and proposals with respect to any negotiable subject or matter.
2. The Employer and the Union agree to waive the right to negotiate with respect to any subject matter referred to or covered in this Agreement for the duration of this contract, unless by mutual consent or as provided in this Agreement.

Section C:

In the event that a state of civil emergency is declared by the Mayor (civil disorder, natural disaster, etc.), the provisions of this Agreement may be suspended during the time of the emergency or activation.

Section D:

If either Party desires to renegotiate, renew or modify the Agreement, it will do so by giving written notice to the other Party on or before March 31 of the year preceding the September termination date. The Agreement may be rolled over for two (2) years.

APPENDIX 1

Exchange of Work Days Form

1. Name of Employee _____
(wanting to swap)

a. Position _____

b. Date/Shift _____

(To be covered by the employee agreeing to take the shift).

I hereby agree to cover the date(s) listed in 2b below for the employee in exchange for him/her covering my dates listed in 1b above.

Employee's Signature

Date

I have been made aware of this swap(s) and approve it.

Supervisor's Signature

Date

2. Name of Employee _____
(covering swap)

a. Position _____

b. Date/Shift _____

(to be covered by the employee agreeing to take the shift).

I hereby agree to cover the dates listed in 1b above for the named employee in exchange for him/her covering my dates listed 2b above.

Employee's Signature

Date

I have been made aware of this swap(s) and approve it.

Supervisor's Signature

Date

APPENDIX 1

HSEMA Rules and Procedures for SWAP

- 1) Neither party can be on leave restriction.
- 2) The exchange must occur within the same week.
- 3) The parties must have like skill sets.
- 4) In the event an employee is unable to report to work as a result of unscheduled leave, he/she must be responsible in finding his/her replacement or alternate.
- 5) If a replacement/alternate cannot be identified, the employee is responsible for reporting to work and carrying out assigned duties.
- 6) If the employee fails to show he/she will be charged an Absence Without Official Leave (AWOL).
- 7) If either party is charged AWOL for failing to report on agreed upon day he/she will be restricted from participating in any future exchange of days for a 12-month period.
- 8) The parties are not utilizing the agreement as a tool for overtime compensation. If either employee has fulfilled an eighty (80) hour pay period, they cannot enter into an agreement during that same pay period.
- 9) Each employee is limited to only six (6) separate exchanges within a twelve (12) month period.
- 10) Each employee is free at the end of the sixth and final agreement during the twelve (12) month period to enter into agreement with any other interested employees that perform like skill sets.
- 11) Both parties understand that each new subsequent agreement with any new employees again is limited to only six (6) separate agreements of exchanging days within a twelve (12) month period.

Date - Week Ending: _____

OFFICIAL TIME REPORT

Agency, Division, Branch _____

Employee Name _____ Union Title _____ Union _____

Name of Supervisor Submitting Report _____

[illegible]

This form shall be administered in accordance with the Collective Bargaining Agreement, including representational functions of official time (Activity) as identified in Article 16. [See Activity List on Reverse Side.] The union representative completes this form and the immediate supervisor will initial the last column. This form is not a time sheet and shall only be used to record the use of official time. Send original to the Office of Labor Relations and Collective Bargaining, with a copy to the supervisor and a copy to the union representative.


REPRESENTATIONAL FUNCTIONS OF OFFICIAL TIME (Activity):


1	Investigation, receipt, preparation and presentation of grievances and safety issues
2	Labor-Management and safety committee meetings
3	Preparation and representation in arbitration, PERB, OEA, OHR and other applicable jurisdictional body
4	Attending meetings with Agency, Mayor, City Council, Congress or other official body
5	Attending negotiation meetings as designated member of team or acting as alternate for absent member
6	Consulting with Agency or its representatives, other Union representatives, or employees, concerning enforcement of Agreement
7	To attend training or other activities to further the interests of improving the Labor-Management relationship
8	Travel to and from any of the activities listed above

FOR THE DISTRICT OF COLUMBIA
GOVERNMENT


Lionel Sims, Director 5/23/2016
Office of Labor Relations and
Collective Bargaining

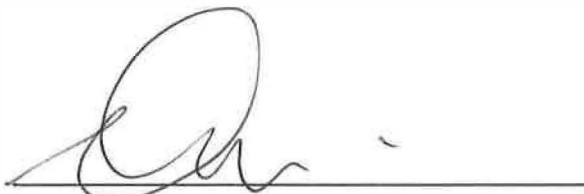

Chris Geldart, Director
Homeland Security and Emergency
Management Agency


Repunzelle Bullock, Esq., Chief Negotiator
Office of Labor Relations and
Collective Bargaining


Brian Baker, Labor Liaison
Homeland Security and Emergency
Management Agency

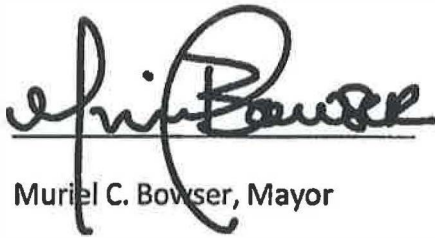
FOR THE NATIONAL ASSOCIATION OF
EMPLOYEES, Local R3-08


Lee Blackmon, National Representative
NAGE


David Hackney, President
NAGE Local R3-08

APPROVAL

This collective bargaining agreement between the District of Columbia Departments of Homeland Security and Emergency Management Agency and the National Association of Government Employees, Local R3-08, dated May 23, 2016 has been reviewed in accordance with §1-617.15 of the District of Columbia Official Code (2001 Ed.) and is hereby approved on this 26th day of May 2016.



Muriel C. Bowser, Mayor

HOMELAND SECURITY COMMISSION

Friday, September 11, 2020

3:00 – 4:30 p.m.

Virtual WebEx Meeting

Commission Member Attendees: Brad Belzak (Chair), Brian Baker, Phil McNamara

HSEMA Attendee(s): Jason Rubinstein (HSEMA)

Invited Attendees: Dr. Gavin Smith, (Professor, UNC Chapple Hill)

(Commissioners open the meeting and provide introductions and participate in moment of silence to commemorate the men and women who served our country on 9/11)

Note: no members of the public are present.

Brad: Thank you very much for being here today, Dr. Smith. Could you please discuss ESF-6 from the national perspective, international perspective, and the State of Mississippi? We appreciate any insights as well as any leading practices.

Dr. Smith: I think about mass care from a different lens, namely under the principle of housing. For example, Hurricane Katrina devastated 50,000 homes. The provision of temporary housing and new permanent housing was a big issue. If there was a true catastrophe in the District of Columbia that destroyed housing units, where would the people go? Considering available housing stock that could serve as temporary or transitional shelter is a big consideration and the delta between different threats. It's important to weigh the potential options to improve the current model. For instance, could voucher programs and federal assistance programs be implemented? Where may they be accessible to the public, and could the District be reimbursed?

In Mississippi, we used to rely on the use of campers and mobile homes to house people for long periods of time. I advocated that we do better than provide campers, because campers are not meant for permanent residents and only have temporary electric systems. So, we submitted a request to congress and obtained a grant to provide modular housing. The housing used a wheeled undercarriage that could be set on a permanent foundation. I bring this example up, because, although it may be out of the box, we could draw lessons learned from the Mississippi Alternative Housing Program. Mississippi did transition back to the camper model, even after we got the grant and implemented the new method. We developed this better idea (modular housing). However, FEMA opposed it. So, we went around them and went to congress. But, after we implemented it once, FEMA just went back to the old model because it was what they knew. So, the institutional resistance was an important lesson learned.

Brian: Do have thoughts on the state of FEMA's current policy posture and the ability to be creative and open to these solutions? In the city, could we turn parking lots into aesthetic areas? Do you see FEMA going in the direction towards innovation?

Dr. Smith: I don't see it as FEMA's strong suit. We were able to move past FEMA initially due to our political structure. However, local governments are often overwhelmed during a disaster, financially, and are required to go back to FEMA's provided structure/methods. Smaller communities often are forced to fall back on what FEMA provides. Having connections to Council is a big asset.

Also, it's important to consider where you place the housing site and make sure they are placed strategically and consider community impact. (For instance, if you use a park, consider where the kids will play).

Another issue I saw in NC and New Orleans was temporary resettlement and bringing people back, post-recovery. (Draws on example of Mayor LaToya Cantrell in New Orleans, who spurred tremendous efforts to preserve a community, post hurricane Katrina).

Brad: The Waterfront in DC used to just be neighborhoods, with little tourism. Now, we have a large thriving community from Georgetown to Alexandria, to the national harbor, to Anacostia, up to the Whitehouse. It's a soft target. Our worry is that the water table is already high.

Dr. Smith: Something you may want to explore is the temporary relocation of residents. For example, if electrical generators are flooded, where would you send the affected populace? In Hurricane Mathew, we developed Land Suitability Analysis. We looked at areas in the town that were appropriate to move people and considered how to sustain the tax base. Distance to schools, roads, available housing, etc., are all related to the buyout. For addition information, I recommend you check out the Hurricane Mathew Disaster Recovery Resilience Initiative and <https://coastalresiliencecenter.unc.edu/>.

Phil: I think we need the report to reflect the importance of pre-planning mass care efforts in the District. We should have mass care prep contemplation pre-disaster and pre-incident. Thank you, Gavin.

Dr. Smith: Pre-event planning is a crucial step, and meeting with your land use planning department. Land use planners say emergency managers don't plan and emergency managers say planners don't operate their plans. The integration is crucial. Transit-oriented development along nodes of subway systems are physically designed for the purpose. In mass care, you ask how you can prepare for the demographic populations and think about the areas that are best suited to relocate.

Phil: The notion of nodes around subway stations really hits a good point. I'm embarrassed to admit, you sent me to google because I didn't know which agency did land use planning in the District. There is an entire office. Did HSEMA ever work with the Office of Planning, Brian?

Brian: It is a close relationship that is built around mitigation, much more so than disaster planning. We were very involved in the city master plan and aligning mitigation dollars. A lot of people don't realize how flood prone DC is. In SW, we built out the city near the Potomac, which is prone to flooding. More focus could be placed if we had to establish temporary housing

sites and address potential displacement. Which areas of the city could we build up and entwine with areas that didn't have opportunities for growth? Involving the Office of Planning on those contingency plans would be very useful.

Phil: I could see us recommending stronger linkage between the Office of Planning and HSEMA.

Brad: On resilience, are there innovations or design principles (from New Zealand or your experience internationally) that we could incorporate in DC?

Dr. Smith: The Hurricane Mathew analysis is worth reviewing. Also, looking at mass care from the lens of new issues, for example, extreme heat. In the early 90s we had people die during a heat wave because they didn't want to leave their homes. The fatalities were preventable. Design issues and psychological issues were the barriers. How are we going to retrofit the big cities to avoid preventable deaths? We want to consider city design, human capital, and incentivize people to go to the cooling center. Considering mobility, mass care and extreme heat in the wake of climate change will be increasingly important.

Brad: I know heat is a big constant issue. Can you speak to exercising?

Dr. Smith: I haven't done a lot of exercise related to mass care. I've done more on recovery. But what I would say is that exercises are often only done with government actors. How often does it engage nonprofits and the private sector? We find out in a disaster (or afterwards) that these groups played a role and would have benefited from being at the table. This also stretches out the recovery and response time.

Brad: Thank you. On COVID, we are facing simultaneous events right now. How do deal with this? Are there any best practices or lessons learned?

Dr. Smith: I have some thoughts on this, looking at collaboration across entities, and from a University setting. We had political pressure to bring students back to UNC. I argued we were not ready, and we spent millions on preparedness measures. I said it would not work. The administration was not listening. We reopened and, in a week, we had 300 cases. Eventually we closed back. We spent millions preparing to be in-person, but our emphasis was misplaced. More relevant to you, it goes back to the issues of temporary housing. It has a technical and social side. How do we convey messages to people to do work for the public good? How do we invest in messaging while also doing things like putting together cubicles and physical infrastructure that keeps people safe? We need both the technical applications and the right messaging.

Thinking about the shelter in place option - like if it's a hurricane, you think about whether you shelter-in-place and if the supporting structure is vulnerable. If your HVAC survives but your generator is in a flood prone area, you could be stuck with no elevator in a 15 story walk up. (Shares experience from Houston where this was a big issue where it impacted losing cancer research). A shelter-in-place approach requires this consideration.

Brad: Thanks so much.

Dr. Smith leaves the call and Commissioners continue the meeting.

Brad: Is 7 jurisdictions enough for this study? (Brian, Brad, and Phil feel it is).

Phil: My question is, if we have 5-6 recommendations we believe in, do we run the risk of DC saying they are already doing those things? Do we need to ask them if they want to give us a presentation?

Brad: Great question. I'm more fervent on the notion of our current direction. I think we can produce a report with very cogent findings. They are for HSEMA, the government at large, and the American people. Drawing in leading best practices for DC from other jurisdictions is the report's emphasis.

Phil: I think you're right. We explain upfront that we made a choice not to interview DC agencies. That's enough of a caveat.

Brian: I think that works. Let's be clear in the report so that it can't be perceived internal to DC (Human Services, or HSEMA, Deputy Mayor, Mayor, Council). We are clear we are not highlighting deficiency; we are highlighting best practices. We just make sure it is presented in that lens.

Commissioners move to end the meeting. No members of the public are present. Meeting is adjourned.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

HOMELAND SECURITY COMMISSION
Thursday, August 20, 2020
4:30 – 5:30 p.m.
Virtual WebEx Meeting

Commission Member Attendees: Brad Belzak (Chair), Ed Pearson, Phil McNamara

HSEMA Attendee(s): Jason Rubinstein (HSEMA)

Invited Attendees: John Scott, President of the Florida Emergency Preparedness Association and Director of Brevard County Homeland Security Emergency Management Agency

Brad: (Opens the meeting, addresses the Homeland Security Commission, and thanks the invited guests for joining and participating).

Note, no members of the public are present.

Phil: (Thanks John for meeting and asks initial question on the strengths and challenges facing Brevard County emergency management).

John: We have run into leadership challenges that require participation and money to get projects completed. When hurricane Mathew struck, it reminded the county of the importance of owning the leadership support responsibility. We built an entire program on a staffing list, disaster role, personnel, availability, exemption processes, etc.

Phil: To clarify, these are the staff that work for you and the agency in Brevard County?

John: We pulled staff from Parks and Rec, Housing Services, Human Resources, Public Works, etc. There was a seismic shift in our program. We began producing shelter kits. We got a warehouse and engaged in cost-benefit analysis. Having the Mass Care Working Group helped us tackle different pieces of our state and local program and collaborate. We uncovered issues such as the American Red Cross' (ARC) potential unavailability and applied policies and practices that permitted our ongoing operations. What we sold our leadership on was the notion that providing safe sheltering was a statutory requirement. We needed to own this and find a way to fulfill our responsibilities.

Phil: How many counties are engaging in response efforts without the usual ARC assistance?

John: Around 60, maybe. We have all repositioned ARC in some shape or form. Everyone has pivoted them in some direction.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

Many ARC staff are just-in-time volunteers. I would love to see ARC spend more time and energy on volunteer recruitment. I think you can see the importance of investing in the volunteers.

Circling back, the ESF #6 is led by Brevard County EM. We put a lot of energy and resources behind the program. We are constantly working to improve. It took us 6 months to build and implement the new program. We didn't start rostering and training people until June, this year. We administered around 25 sheltering trainings since then. We are still bare bones, but we do a good job with what we have. An activation would present challenges. Hurricane Irma came before we were ready, however, I was proud of our efforts. Shelter and notification processes were not perfect, but overall, we did a good job.

Brad: What changes did you make to the program?

John: We ensured there was a surplus of staff. Sheltering is never a problem until it is. The breakdown never arises at a convenient time. A big point of emphasis was to have more staff on site than we needed. The second priority was to instill values in the training that drives the heart of the mission by connecting the worker to the mission and the mission to the resident. We preach the staff being there as advocates and we try to compensate them well for their efforts. We want the staff to know they are there to assist residents who are having a bad day and emphasize the importance of their empathy and kindness.

Brad: That was helpful, thank you. Are you using any technology? Any applications?

John: I am old school. I don't always like technology in these kinds of situations. When tech breaks down, people shut down. We still do paper registration on index cards and we just capture core information. We have the client tell us medical information, allergy information, etc.

When it comes to client interaction, Covid makes it challenging. We have an application but I'm not a huge fan of it. The group that needs relocation during hurricanes is not usually the savviest with technology nor do they always have access to the application. I believe people talking to people is the better approach in many circumstances.

Brad: Can you talk about training and exercising?

John: We haven't done any exercises for the actual program, but we do it live, in practice. In terms of who is involved, we try to keep political folks separate from the operators. From an exercise standpoint, we understand both sides of the issue. Operationally, here is how we open shelters, and politically, here is why. It's about knowing the community and the demographic, locations of populations, pockets of poverty, underserved populations, etc.

Brad: Do you engage in data analytics and do you think you could be more efficient if you focused on demographics?

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

John: One thing I think would be critical to consider is behavioral analysis. We saw a theme in Hurricane Mathew and Irma. If the storm is here in 5 days, our phone goes crazy on day 5. You would think we never even heard of opening a shelter, based on the calls. There is a large artificial demand. But when we open the shelter, people don't go. We will get maybe 1200 calls to register and then when we would call to provide pick up, the person would decline, last minute. We had one person crying to get into a special needs shelter. Then, right before we came to get her, she declined. So many people just want to make sure they are on the list. I would love to see more data on this trend.

Brad: That is very interesting. Would you say that the biggest issue is false calls?

John: Yes, for me.

Phil: I want to take advantage of your expertise from your FEPA role. If you were to channel some of the top challenges that other FEPA members would face, what do you think the top one or two challenges would be?

John: Everyone would say staffing is the number one issue. Second is access to resources. Some of the resource issue would be driven by geographic limitations, size of the program, etc. For example, some of our best shelters don't have a generator. Each generator costs half a million dollars.

Phil: How do you balance the interest of people's comfort? Doesn't loss of power contribute to that?

John: Yes. We try our best to be clear about expectations. Our experience is 'alive in and alive out' and 'same condition in and same condition out'. We tell people they are not guaranteed power. It's very hard to get FEMA money approved for power generators. There is no money for enhancing a person's experience. The disparity is that the underserved areas tend to be where shelters are unavailable. *(John also provides issue of people not wanting to leave pets behind).* Pets are evacuation decision makers.

Phil: *(Emphasizes this line).*

John: Having pet friendly shelters are crucial. Down the line we would like them to all be made pet friendly.

John: I looked over your questions and would like to offer some general responses. We are doing congregate sheltering. Non-congregate is obviously preferred right now, but it does limit our ability to be creative. Using local dollars now to do things virtually on a more permanent basis may become the norm. In terms of disaster housing, it is the single biggest barrier to recovery.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

There is no good program solution for that. From a policy standpoint, disaster housing is discussed, but never serviced. We are trying to use Covid as a chance to reinvest our program, strategically. I think we should set up recovery strategies. Establishing building codes and finding ways to take bad housing practices and replacing them with a better structure would be preferred. We shouldn't have to evacuate as many people, because they should be housed in a location where they are secure.

Brad: Thank you very much.

Meeting adjourned. Note, no members of the public are present.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

HOMELAND SECURITY COMMISSION

Thursday, August 13, 2020

3:00 – 5:00 p.m.

Virtual WebEx Meeting

Commission Member Attendees: Brad Belzak (Chair), Joanna Turner (joined from 3 - 4:30 pm), Ed Pearson (joined at 4 pm), Brian Baker (joined from 3 - 4 pm)

HSEMA Attendee(s): Chris White, Dion Black, Jason Rubinstein

Invited Attendees: Bryan Koon, VP of HSEM at IEM and former Director at the Florida Division of Emergency Management; Inaki Rezola, Operations Section Chief, Hillsborough County Fire Rescue, Office of Emergency Management, Tampa, FL

Brad: (Opens the meeting, addresses the Homeland Security Commission, and thanks the invited guests for joining and participating).

Note, no members of the public are present.

Bryan: In the State of Florida we have been activated for roughly 6 months. On the plus side, we are operating as a well-oiled machine. However, certainly an issue now is staff fatigue. This year, the ability to shelter people using past models is reduced due to social distancing. Personnel who would operate the shelters are also reduced because of COVID. In some cases, the volunteers are from among the older population, who are at higher risk.

Trying to be more surgical on evacuation technique is a big priority. Hurricane forecasts are still prone to error. Fortunately, we have generally erred on the side of extreme caution as it applies to evacuation.

Looking ahead, extra caution is needed and it's important to communicate to the general public about which evacuation zones they are in. Campaigns are underway to educate on evacuation zones and home safety assessments based on location in the state. Educating people to help them make better decisions (whether to evacuate) is the goal.

The other challenge is convincing some people to go to a shelter where there is potential congregation and explain why it's the best choice as opposed to staying in their home. That is the challenge the state is facing. Evacuation occurs at the county level, but it is everyone's interest to have consolidated information on a state and local level. This integrates policy makers, police, public officials, and the people. It calls for massive coordination and it is a giant logistical challenge. Executing this in real time is also a challenge. A lot of what we will do in hurricane

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

season this year will be done without a practice run or exercise. The issue is, counties may typically have 20 shelters, but, during a storm, we would consolidate to use only a few. However, the interest in letting people spread out due to COVID would incline us to run more shelters.

Also, the demand to use shelters is likely to be higher due to job loss and challenges related to loss of income. We anticipate greater demand, especially as unemployment benefits run out.

Brian: Based upon your national perspective, are there any best practices coming out for sheltering people with special needs or moving skilled nursing facilities? What should we be thinking about?

Bryan: As a government, you want to clamp down and make sure they have real executable plans in place. One of the priorities we have in Florida is to make sure everyone knows the plan and that it is useable. Also, we want to make sure we are offering healthcare services and providing essential care. Transportation is also a challenging issue. We want to make sure we are only transporting vulnerable populations as needed.

Joanna: Mass care has become increasingly more complicated in the wake of the pandemic. You mentioned that the staff in Florida are working crisis after crisis. As you operationalize these plans, the question is, how do we keep people's eye on the prize?

Bryan: People will respond to inertia and momentum. That will get them through a few days or a week, but beyond that, it becomes a challenge. You must give people a break so they can recuperate. Hiring temporary staff support is something one should consider.

Citizens are also suffering from fatigue from the constant bad news and are facing mental health challenges. You must keep your pulse on society. For instance, people's receptiveness to evacuating will depend on their previous experience evacuating. It's about establishing empathy and connection. You also want to keep in mind the stress of schools coming back online and all other compounding stressors. You should keep in mind that messaging may need to evolve week by week.

Joanna: We should see if the Mayor needs statutory authority to deputize staff for mass care events. (Internal note for HSEMA follow up).

Joanna: Bryan, you raised a key transportation issue. How do you convince people to stay put or leave?

Bryan: It is a part of messaging and asking nicely. You can't really use law enforcement to stop people from getting in their car. Response is really driven by messaging. Also, in Florida, our assumption is that even in a bad storm, we may only get half the requested population to evacuate. We also have various strategies for the evacuation itself, such as opening the shoulder

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

lane. You can only do this below a certain speed and go one-way on the interstate. However, everyone hates the one-way option. Even though it adds capacity, it sucks up a large portion of law enforcement personnel.

Joanna: Thank you.

Brad: in terms of resiliency, in DC we are becoming increasingly focused on the waterfront. Now, it is one of the east coast's greatest locations to visit. It also poses some significant concerns due to flooding. Could you share best practices on resiliency you have used in Florida?

Bryan: There are a few things I've seen that were successful. I've always aimed to increase desire for people to choose a better option. (Draws example of air bags and seat belts). You are starting to see this implemented in Miami. Consumer demand is pushing the issue on enforcement for building codes and general infrastructure requirements to be above the flood zone. Mitigation investments save time and money in the long run. FEMA, for example, has an enhanced mitigation program that awards strong state plans with grant incentives.

Brad: (Thanks Mr. Bryan Koon for his time).

Inaki Rezola joins the meeting.

(Commission provides introductions).

Joanna: Thank you for meeting with us. Can you speak about the impact of COVID on your ESF 6 plan?

Inaki: In Tampa, we rank high in terms of catastrophic hurricanes. We are up there with New Orleans and New York City. We can have up to 30 ft of storm surge in this type of scenario.

FEMA's guidance says for risk sheltering you need 60 square feet per person. Risk space is limited to begin with. Now, it's a matter of whether we can still make space and adjust for COVID. We looked at previous shelter registration data. Most people do not evacuate by themselves. They go with loved ones or family. We developed a formula that says everyone gets a certain amount of square feet in the shelter. For families, we are considering the model of adding 20 square feet per family member. Through this approach, we are revising our old model to accommodate families being together while being efficient with space. Also, our goal is to screen people coming in so if they come in with symptoms, we try to isolate them and shelter them. Taking additional precautions like using hand sanitizer, individual food packaging, etc., are all added steps we are taking. If our numbers go up from a shelter, on the back side, we can encourage non-congregate options (such as using hotels). There are other challenges. In terms of transportation, we have had some resistance. Every day we learn something new that we actively work to apply, like using water bottles in school instead of faucets (to account for issues related

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

to water contamination). Schools are trying to transition away from water fountains to the devices used to refill water bottles.

In addition, we are focused on post-disaster planning. The Red Cross says they can't support a shelter with more than 50 people. From our end, it is hard to meet the sheltering need with many small shelters.

Brad: Regarding the issue with Red Cross, is that an issue of the Red Cross not willing to staff? How do you mitigate this when they won't staff a shelter with over 50 people?

Inaki: The shortage of resources to take care of people is also a part of the issue. So, the question is how you manage a potentially deadly virus when people are still hurting? We still must open shelters. We must evacuate them from hurricane zones.

Joanna: Where did you come up with the 60 square feet per person calculation?

Inaki: We developed that based on our data inventory. We found that people often came to shelters together. We could accommodate the desire for people to stay together and be efficient with space. We used data to determine the additional 20 square feet added to the initial 60 square feet would be enough.

A cruise ship setting is a perfect example for comparing sheltering in the context of COVID. If the ship is sinking, everyone is getting on a lifeboat, regardless of COVID. We must think about the same notion in the context of catastrophic events.

Brad: We are never accounting for simultaneous catastrophic events. Very few will allocate budget for that. We always must do more with less. Especially when it's a one in one hundred-year storm.

Inaki: At the end of the day, we must mitigate and think about how we can serve the people and respond effectively. There are things we can do as a community from a mitigation standpoint. But, when your homes are devastated, how do you deal with it?

Brad: We are looking for innovative approaches. (Mentions Deaf Link app). Do you have any tech. approaches you may recommend?

Bryan: Right now, the state has a company working on an app for non-congregate sheltering. We have been giving them technical guidance. We have professors helping us develop shelter registration applications. We are working with both in tandem.

Brad: Can you speak further about the app.?

Inaki: It removes the element of registering for shelters, in person. The goal would be to allow shelter registration without paper. Then, when you get to the shelter, all you do is check in. Then,

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security and Emergency Management Agency

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

we are transmitting the individual's info in our EOC so we can track populations, manage resources, occupancy, and so forth.

Brad: Will the app use data analysis? How expansive is that?

Inaki: We would tie it into our heat map. Again, right now we are trying to build this out. The non-congregate app is one we are trying to apply for shelter use. But again, if we opened shelters tomorrow, it would have to be paper registration. If we opened shelters 2 months from now, that may be the time we need.

Brad: Thank you so much for your time.

Meet is briefly reopened to the public. No members of the public are present. Meeting is adjourned.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

HOMELAND SECURITY COMMISSION
QUARTERLY MEETING

Thursday, August 6, 2020
3:00 pm to 5:00 pm
Virtual Webex Meeting

Commission Member Attendees: Brad Belzak (Chair), Phil McNamara, Brian Baker

HSEMA Attendee(s): Dion Black, Jason Rubinstein, Ronit D. (HSEMA Intern), Caitlin A. (HSEMA Intern), Natalie R. (HSEMA Intern).

Invited Attendees: Holly Porter, Deputy Chief Administrative Officer for the County of San Diego and Julie Jeakle, Senior Emergency Services Coordinator at County of San Diego Office of Emergency Services; Lisa Jones, Director of Homeland Security and Emergency Management for the city of Phoenix, Arizona.

Brad: (Opens the meeting, addresses the Homeland Security Commission, and thanks the invited guests for joining and participating).

Note, no members of the public are present.

Brad: Could you please talk about the strengths and challenges of your ESF-6 plan?

Julie: It covers sheltering, feeding, and bulk resource distribution. We are very heavy on the feeding side. We anticipate disasters that occur every year so we have a lot of practice in implementing ESF-6.

The types of disasters often impact cross-jurisdictions. It's more than just a county initiative, so we aim to address that reality in our mass care plan. This highlights the joint role our cities play. American Red Cross (ARC) is also a very strong partner. We have adopted protocols and procedures with respect to this. We have all adopted ARC protocols, procedures, guidelines and standards when it comes to our mass care programs. We interact and engage to provide strong service to our residents who are impacted by disasters. For example, we had a largescale fire in 2007, it was catastrophic, people were evacuated, and there were 45 emergency shelters open simultaneously with 20,000 people. This is what we use as our baseline planning at the end of the day. We plan to be able to shelter 20,000 people. Fortunately, we haven't had a large incident of that scope and scale since then, but we had a lot of smaller incidents that have really tested our systems. We know we're on the right path. We take access and functional needs planning very seriously as all jurisdictions reasonably should to make sure the level of care or support is in

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

place. We have a county shelter program, and disaster rapid assessment teams with specialties in health service areas.

Phil: When you send the disaster assessment team out to a county run facility are you essentially sending one part of County staff to look at how another part of County staff operate? Can you speak more about this?

Julie: We have community members arriving to the shelters before they are even open. Our team is trying to get the doors open in an emergent event. The disaster rapid assessment team is not designed to look at the work of our employees, it's designed to look at the unique needs of the people who are in that shelter and the population coming in.

Phil: Thank you, I appreciate that context. Brian, does HSEMA do something similar?

Brian: Our threats in DC are often not whole communities, though HSEMA and DHS partner with their teams to service populations (draws on Arthur Capper as example).

Have you made changes to your program to meet the challenges of moving towards a non-congregate shelter environment?

Julie: We are in the middle of those planning efforts and I will say that the more we dig in, the more we realized how complex of an issue this is. We meet with Red Cross weekly and the protocols are constantly changing. In the last two weeks we have tried to wrap our heads around what non-congregate sheltering would look like if we had a very fast-moving wildfire. The ARC in Southern California has responded to two significant wildfires in the last two weeks where they kind of tested some of their new protocols related to non-congregate sheltering. We have concerns about their ability to get people out in a timely way.

Brad: Can you hit the high points on the ways you are preparing and the challenges you face?

Holly: Our hotels are likely a part of the solution. We do know that most ARC volunteers may not be available immediately, which is a challenge. ARC gave a presentation and said they would be able to assist us and have the capacity with their volunteer force to shelter 20,000 individuals. We consider this capacity in our preparation.

Julie: Regarding ARC local capabilities, I think they're starting to realize that while they look very good on paper, in practice there are very significant gaps. ARC national protocols say they will not house more than 350 people in a facility. To get to 350 people you must have 50,000 square feet, which is a substantial facility, and they have one disaster health service member who is available to assist, in person.

Brad: Can you speak about ESF-6 from the lens of innovative technology?

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

Holly: The County Fire Department is using a software program to assist locating vehicles. We also store the regional wildland fire safety plans, as well as critical infrastructure mapping products. This allows the ability to share information from the field with the emergency operations center (EOC). The technology allows us to map out a large geographic area. We use cameras to zoom in to an area when there is a fire, and we can get a bird's eye view on what's happening throughout our rural areas.

Julie: We are working with our public health partners to use the data they are mapping, related to individuals who are Covid positive, to consider for evacuation planning. We do have assessment forms that these teams utilized that we designed, in-house. They look at very specific areas and send that information to the EOC so they can get flagged, right away, and either get resources or equipment.

Phil: Do elected officials ever have an opportunity to exercise?

Holly: Every other year we have an original full-scale exercise and we invite the chair of our Board of Supervisors into our EOC.

Julie: *(Speaks about the functional exercise).*

Phil: Thank you, both.

Holly: I think we have a couple minutes left. Can we talk a little bit about the feeding task force?

Julie: Feeding is a major issue anywhere, especially when you're dealing with thousands of people potentially who need assistance. In addition to community churches and ARC, we also worked closely with our private industry partners, like Cisco. If there is a large incident, we can activate a special task force that can immediately get on conference calls and start rolling out into the structure of a program that serves up to 5000 meals. We funnel through the ARC as an NGO so we don't get caught up in all the government red tape that that may cause undue delays in service. We have a feeding coordinator position in the EOC that coordinates directly with ARC.

Brad: This is exactly what we're looking for and this is very exciting to hear.

Julie: I'd be happy to send you the list of participating agencies. Again, it's the Cisco US Foods as our private partner. We work very closely with our food banks. We have Meals on Wheels and we also work with senior transportation providers who might not necessarily be in the food delivery business, but they certainly could be, and they have connections with other entities that that may have refrigerator trucks. Temperature is always a key consideration.

Holly signs off.

Phil: I'm so intrigued by the draft disaster rapid assessment team. You said you were creating apps that use forms to assess feeding needs?

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

Julie: There's four different forms. Each form is looking at something different. We have one that's looking at just the facility, one looks at ADA compliance, one looks at behavioral health as it relates to sheltering needs, and the last one has to do with communications and messaging.

Brad; Thank you. We would love to see the draft disaster rapid assessment team resources and any others from the feeding task force. Anything you have on that that is open source is much appreciated.

Julie: No problem.

Julie signs off.

Lisa Jones joins the conversation. Please note her presentation includes a slide show shared prior to the meeting.

Lisa: (Provides introduction and background on Phoenix).

Brad: With climate change we are having more severe weather frequency. How we can account for this from a planning side?

Lisa: I don't believe a plan can cover everything. I think we must be able to look at what our current plan is in a scaled down version, and then consider what it would like to implement if a huge disaster was also happening. (References slides).

Brad: You mentioned Disability Rights Advocates (DRA) and BCFS Health and Human Services. Can you speak more to their support roles?

Lisa: DRA is supporting a person with a disability and makes sure their needs are covered, and that the government is compliant with those requirements. (*Speaks to extreme heat incidents and examples of accommodating high rises with X number of wheelchair ramps and lifts*).

I believe more than just during operational periods; people need to be at the table for us to have a successful response. (*Draws on lessons learned from Hurricane Harvey and Irma*). We need coordination between the operators and the political actors in the planning, otherwise it promulgates a “let's get it done and ask for ask for permission later” mentality.

(*Addresses slide that describes ESF-6 management structure and exercises*). Sports arenas are used for mass care sheltering, as well the Convention Center. GIS is used for mass care shelter planning and exercises. We also work closely with Red Cross is establish an ADA complaint evaluation.

In my last activation we had a power failure downtown with two older adult facilities. It was 150 degrees. Many refused to leave and so we had to get portable coolers, food, and medical

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

assistance and two ambulances to that location. For the other location, we had to offer emergency assistance, bring in supplies and provide temporary shelter. This is highlighted in the after-action report I shared. The last national level exercise we did in 2018 highlighted, among other things, the importance of staff training on access and functional needs and supporting people with disabilities.

Ronit: How do you fit tribal relations in to your planning?

Lisa: We always include tribal relations as an important aspect of our planning. We have this integrated as a part of our Emergency Management subcommittee.

Brad: Thank you for putting this presentation together.

Note, no members of the public are present.

Meeting adjourned

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

HOMELAND SECURITY COMMISSION
QUARTERLY MEETING

Friday, July 31, 2020
3:00 pm to 5:00 pm
Virtual Webex Meeting

Commission Member Attendees: Brad Belzak (Chair), Phil McNamara, Joanna Turner, and Ed Pearson, Brian Baker

HSEMA Attendee(s): Dion Black, Jason Rubinstein, Ronit D. (HSEMA Intern), Caitlin A. (HSEMA Intern), Natalie R. (HSEMA Intern).

Invited Attendees from the Office of Homeland Security and Emergency Management for the city of Austin, Texas: Juan Ortiz, Director; Bill Wilson, Chief Emergency Plans Officer; Eric Carter (Chief Emergency Management Coordinator for Travis County, Texas).

Seattle Emergency Management Agency: Barb Graff (Former Director)

Brad: (Opens the meeting and addresses the Homeland Security Commission).

Good afternoon. We have quorum and are ready to proceed. Today is July 31, 2020. This meeting of the Homeland Security Commission is kicked off. We are proud to have distinguished guests from the Emergency Management Agency of Austin Texas with us. They are assisting us with our study and examination of ESF-6. We are currently in an open meeting. We would like to move into closed session for the briefing.

Jason: May I ask if there is anyone from the public here. If so, please announce yourself.

(Commissioners unanimously vote to close the meeting).

Note: No members of the public were present

Meet is briefly reopened to the public. No members of the public are present. Meeting is adjourned.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

HOMELAND SECURITY COMMISSION
QUARTERLY MEETING

Friday, July 10, 2020
3:00 pm to 5:00 pm
Virtual Webex Meeting

Commission Member Attendees: Brad Belzak (Chair), Brian Baker, Phil McNamara, Joanna Turner, and Ed Pearson

HSEMA Attendee(s): Dion Black, Jason Rubinstein

Additional Attendees: Dr. Dennis Onieal

Note: No members of the public were present

Brad: (Opens the meeting and addresses the Homeland Security Commission).

We are pleased to have Dr. Dennis Onieal with us today to provide an overview for our study. Dr. Onieal, thank you for taking time with us and offering insights from your lengthy experience. We appreciate your perspective on mass care and resiliency. Before we get underway, can we have brief introductions?

(Commissioners and meeting attendees introduce themselves).

Jason: I'm not seeing any members of the public present. Do Commissioners wish to move into closed session for Dr. Onieal's briefing?

(Commission does not vote to move into closed session).

Dr. Onieal: I appreciate hearing everyone's background and connections. I'm happy to be here. Emergency Support Function 6 issues rely on a multi-agency and stakeholder response. The response plan is lengthy and thorough. Before I met Brad during our work with Katrina, I supported response efforts for Hurricane Sandy, 9/11, and many other incidents. The success in administering support functions fall on the people engaging in the emergency response operations, and it hinges on their familiarity with the process. My questions to the Commissioners are – What do you want to see? What are you looking to accomplish with the study? What are you worried about and what needs to be taken care of?

Brian: I appreciate the question. I would like us to provide objective recommendations that the District can use to approach mass care in a manner that considers the unique environment we are in today. I spent many years with HSEMA, developing the plans you mentioned. I remember

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

when we didn't have a mass care response plan. The plan only came to fruition after Katrina, when we received survivors in the District that we sheltered. The aftermath of sheltering those survivors drove the priority to have a mass care and sheltering plan. Since then, a lot of those original players are no longer a part of the plan, and a lot of the assumptions (such as congregate sheltering), no longer carry the same consideration. As we look back, we need to develop plans that can be executed, considering the elements and situations that are at hand. I want a plan that can be pulled off the shelf. As a Commission, we need to produce a report that connects the expertise and information, so it is usable, today.

Ed: I echo the sentiment Brian has expressed. I want recommendations that are usable and tangible for the District. (Draws on Arthur Capper as example of modern incident that prompts an adapted mass care response plan). Having worked in the fire service, I know resources were put forth to HSEMA, DC Fire and many other agencies to empower a mass care response. I believe we can do better. I want to develop tangible recommendations that can improve upon our current framework.

Dion: Thank you for the opportunity to weigh in. My role is to support your mission as HSEMA's General Counsel. I am supposed to stay impartial and support in any way I can. I understand that mass care has been a very crucial issue for the District. I look forward to taking in what you provide.

Joanna: I want us to have actionable recommendations. I don't want to pile on or offer redundant guidance. We have a world class city, with world class leadership and appointees. I want us to do the research, exam gaps, and provide recommendations on how to fill those gaps. I don't want this project to be in a vacuum. Although the Commission has worked on pandemics before, this is a new reality we live in. Even when we are through this pandemic, we recognize that the globe will see more. I want to see adaptive and actionable plans that account for exigent and broad circumstances.

Phil: I want to connect with other governments and entities around the country and learn from them. The mass care plan in our District was developed through a lot of time and attention. We should assess gaps in the current plan, identify information that is missing, and capture best practices from other units within the government. When we talk about actionable recommendations we should consider when the plan was last utilized. I would love to see a TTX or example of when the mass care plan was last implemented. Has it been done on the Mayor's level, Operational level, etc.?

Dr. Onieal: (Thanks Commissioners for their initial feedback and asks about the Arthur Capper Fire).

Brian: Arthur Capper highlighted that the District would benefit from additional information and plans for addressing mass care incidents, specifically in servicing vulnerable populations. This

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

incident posed challenges for the supporting agencies and called for a deep look in sheltering and mass care from a broad perspective.

Ed: The fire occurred just before I retired.

Joanna: September 2018 was the date of the fire.

Ed: We ended up with a challenge that was a bit unexpected - to service the displaced residents of a vulnerable population. A high-rise fire and large-scale displacement presented a unique issue. They had to search, recover residents, do recon - I believe they found one resident days after the incident.

Dr. Onieal: Before we look for the silver bullet, we should consider the basics. Relocating displaced residents after a fire should be a manageable issue for DC. When the planes crashed into the pentagon and the Potomac river, the displacement was simple. Had those planes crashed into a neighborhood; the relocation would have been vastly complex. I can provide you with people to talk to from various cities who could offer additional perspective. Circling back, the first questions regarding the mass care plan would be - are you familiar with the plan, and when did you last exercise it? I bet it would take some time to find the actual plan and become familiar with it. Brian, do you agree?

Brian: I agree. Plans are not always socialized to leadership. They are developed by planners. At times, the operators do not know what's in the plan or where it is.

Dr. Onieal: If the politicians aren't familiar with the plan itself, they will make political decisions as opposed to emergency management decisions. We see this in the federal service. In the emerging situations and circumstances, politicians look for solutions that override the civil service. Making sure those with authority do not look past the service component is an important gap to fill.

Brad: I want to know how cities are dealing with the pandemic while planning for emerging issues, such as hurricanes and severe weather. What steps are they taking? When did they last exercise their plan? Also, are first responders equipped to respond to events during a pandemic? Do they have the gear and equipment?

Next, what is the gold standard? What makes a plan successful? Another concern I have is the resiliency of the waterfront. DC Council is also concerned about relocation and displacement issues at the waterfront. Lastly, how do we deal with the vulnerable populations in the context of relocation, the pandemic, mass care, etc.

Dr. Onieal: Vulnerable populations face a disparate impact in the wake of pandemics and natural disasters. How can those without credit and readily available finances ensure security during

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

these disasters? Again, I urge us not to look for the silver bullet. We want to make sure those who are executing the plan are familiar with it. We want this familiarity ahead of the incident. That is the current biggest vulnerability I see.

Brad: I also want us to look at innovation. We should see what cities around the world are doing differently, and how we can leverage that information in the District's planning. I would like us to consider a layered approach. To your point, Dr. Onieal, there is no silver bullet, but I'm hoping our work can contribute in a meaningful way to the information that is available.

Dr. Onieal: I am available any time. I will get back to you with additional contacts that may assist you in your research.

Brad: Thank you for taking the time. We love your insights and will follow up.

(Dr. Onieal signs off).

Do we need to stay open or closed?

Dion: If we move into closed session, let's make a note in the minutes indicating that we did so, provide the basis for moving into closed session, and assign the permissible reason.

Commission unanimously votes to close the meeting at 3:48 pm, pursuant to D.C. Code §2-575(b)(8), 7-2271.04, and 7-2271.05, in the interest of preserving public health and safety.

***Meeting briefly reopens at approximately 4:35 pm. No members of the public are present.
Meeting adjourned.***

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

HOMELAND SECURITY COMMISSION
QUARTERLY MEETING

Wednesday, June 10, 2020
2:00 pm to 3:30 pm
Virtual Webex Meeting

Commission Member Attendees: Brad Belzak (Chair), Brian Baker, Phil McNamara, and Ed Pearson

HSEMA Attendee(s): Chris White (Deputy Director), Dion Black, Jason Rubinstein

Additional Attendees: Jamie Gorosh (Legislative Counsel, Committee on the Judiciary and Public Safety)

Note: No members of the public were present

Brad: (Opens the meeting, provides introductions and addresses the Commission)

I would just like to take a moment current event. These events represent a significant human rights issue. Beyond anything, people should get out, march, and reform. However, Looting is uncalled for. The city and the Mayor done a great job navigating this.

We as Commissioners are here as advisors and will do more. Let's take this meeting to address each other, talk about the Unity March, state of protests, and of course COVID-19. The Commission is here to sift through the information and misinformation and put in data driven proposals. Let's start with introductions to get the meeting started.

Brian Baker: I would just like to say that through these times I've been very proud to be a DC Resident. DC Fire, HSEMA, DC Council and all contributing agencies have done an incredible job supporting the March, keeping the city safe, and balancing this during COVID-19 response. Chris White, if you could pass on to your agency and members of public safety a big thanks for all the continued work you have been doing. I know its been a lot of sleepless nights around the clock, and your efforts are having a very positive impact.

Phil: I echo the major kudos to the Mayor, Director Rodriguez, HSEMA, and DC Department of Health. Everyone since mid-March has been going over and beyond on coronavirus pandemic response and a public safety response that has facilitated and narrated very peaceful protests. This has been literally one incident after another. A huge thanks to everyone on the front line and supporting during these times. I came down on sixteenth street and saw the "Black Lives Matter" message, in person. It was very moving. Thank you, again.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

Brad: Chris can you give us a snapshot of where we are from HSEMA's side and the District response?

Chris White: (Thanks the group and confirms who is on the call).

We just entered month 4 of activation. The EOC is set up at the DC Health building. It has been a good experience and we have really come together. As a District, we went into phase 1 of reopening on May 29. Over this time, we have seen general decline in new cases. In the past 2 days we saw a small increase, but overall, the trend has been very positive. We do believe we are on the other side of the curve and can proceed to dial up steady-state services. From a public health perspective, things have been trending in right direction. In terms of phase 2, we are thinking about metrics tracking.

Here are the key metrics we consider:

1. Community Spread
2. Transmission Rate
3. Case Positivity Rate
4. Health Service Capacity

Again, we are progressing in the right direction, but we are still looking to maintain sustained decreases in transmission rates, rates of positive cases, and community spread over an extended period. That is the focus of our set up. Operationally, we are expanding testing and now can do so with less restrictions. We have 15 sites around town, including three public sites. We have several firehouses and walk in locations that may be tested within regular core hours during the week. We are doing roughly 400 tests a day. There has been increased demand for testing since the protests and we will be assessing that impact on the overall public health situation.

Looking ahead, in terms of contact tracing- our goal is to get 800-900 contact tracers. We are pushing government employees to take training so we can also leverage our workforce in this effort. That is the summary in a nutshell. We also have roughly 13 grocery distribution sites. School systems are providing sites around the city to provide meals for students and the community. Essential food lines have multiple continued efforts for the foreseeable future.

In terms of isolation quarantine facilities, we have hotels for housing folks within vulnerable population and people experiencing homelessness. Again, the strategy has been to avoid clusters within the homeless population. For recovery operations, folks are tracking the federal buckets of money to make sure we are aware of what is available and needed financially. Our planning team is working with the Reopen DC Committee and we are actively working with each agency to track costs.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

In terms of operations, we are focused on cost recovery and we have a team of folks tracking the federal streams of money to ensure we are charging expenses correctly and efficiently. To sum it up we built an organization that at large is working well and is staffed appropriately. The big question is how long is this going to go on?

We are not making adjustments to our current posture but are poised to do so if needed. We acknowledge the potential of having a second wave and we are in this fight for the foreseeable future. We think about keeping staff focused and motivated. I'm very proud of our staff and city response.

To comment on the protests and our recent posture, the 1st amendment activity has been the focus over the last week and half. MPD is the key law enforcement agency and we are supporting in any way we can.

Phil: Thank you. One observation is just a big hats-off to HSEMA and please pass this sentiment along. The coronavirus.dc.gov website is phenomenal. It is very user friendly. I go at least a few times a week. Please pass long my appreciation for the efforts that are going into that site. On the metrics you discussed, I wanted to comment on how we get from phase 1 to 2, obviously hinged on a decrease in community spread and keeping a low transmission rate. One thing that I don't have as much clarity on is the contact tracing. At one point we heard the District is trying to bring on 900 or so contact tracers. Can you speak a bit to that? And before you go into discussion on Black Lives Matter, I would like to know your perspective on the height of coronavirus response in April. Just maybe if you could give how you feel about your ability back then to take on a planned or unplanned incident, in tandem with hurricane season.

Chris: (Speaks a bit about contract tracing, protests, and hurricane season).

Brad: Just to touch back on mass care. We recognize the city is putting up temporary housing and leverage the convention center. Whatever happens, we are still going to need additional capacity. New development is good, but we are losing homeless shelters to new condos and space to care for people who are especially vulnerable. We also have regular concerns outside of COVID- such as the pure resiliency efforts needed to respond to waterfront flooding and displacement. What is our issue, what is Maryland along the waterfront?

Circling back to our study, I propose the following:

1. We stay the course, looking at resiliency and mass care in lens of catastrophic events.
2. Let's think about how we want to do this study. We are not trying to get in the way of first responders. I was happy we were able to reopen up as a Commission. One reason I didn't push sooner is because I wanted to preserve first responder bandwidth. That said I'm open suggestions on how we can press forward as a commission while balancing this interest.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

Phil: So, how can we be impactful without getting in the way? We could approach it from the perspective of inviting in folks from outside of DC or other cities or states and that did a remarkable job to develop mass care responsibilities. I would have to rely on Brian or Chris White from HSEMA to navigate these contacts. We could invite 2 or 3 of them to get expertise to get what our county has done. The idea is to leverage perspectives of those outside the District. We could also do, similar to what auditors do - a paper examination. See mass care policies, plans and playbook. We could review the papers and procedures. Those are two ideas I would propose.

Also, if this is going to take us 4 months to do - maybe we cycle it to bring in the District in the latter two months.

Brian: I think that approach makes a lot of sense. We want them to be impactful and think about how we offer something that can be used? There is actually a decent amount of money provided through federal agencies (FEMA, HUD, etc.). Can our study include recommendations about what the District can do to improve mass care and improve resilience ahead of next disaster? We can assess resources, what we have in front of us, and propose ideas on funding. Can we take a report and include in HUD applications of other reports? Maybe we as a body can supplement those efforts through our study.

Brad: We also we use the port authority models, mass ports, and others that speak to resiliency, as we assess the impact.

Let's think about this after the call and share our contacts. Let's do a hybrid, with non-DC and DC entities. Having the anecdotal information and seeing some disaster plans and temporary housing plans can supplement our study. We can do a cursory review and a gap analysis. As an example, doing reviews of key cities such as LA, NY and other major markets, and certainly DC. Let's do out-of-state first and then in state as our order-of-operations. I'd like to get a report that's actionable and is something we can get coordinated and distributed quickly. We will use a combo of interviews and data and lessons learned.

Brian: I like that approach.

Brad: We will lay this out in an email, and we will have vote and concur if Jason and Dion are fine with this from the administration side.

Jason: Id recommend we take yours and Brian's vote now, and we do the remaining via email, if Dion agrees? We can use this approve minutes from the last meeting, as well.

Dion: Yes, we can make record of the motion on the floor and use email as electronic means to complete the votes. This way, we are achieving quorum to make the final decision.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

Brad: So, we can vote today and make the plan proposal, and then ask the remaining commission members to vote so we can come to final decision and consensus. Is that allowable?

Dion: Yes. This will allow the final decision to be made with quorum, as required.

Brad: Great. Here is outline moving forward – we vote to proceed with the report, examining resilience and how prepared we are in the city. We are looking at this from a mass care lens with resilience undertone.

Brian: I concur.

Brad: Second, the report length. I think it should be long enough to have an impact and enough substance, but short enough to get it done and for it be digestible. Does 4-6 pages work?

Brian: I think that works.

Brad: In terms of completion schedule, it's a short report. It depends how soon we get meetings on the calendar and synthesize information. What is a fair date? I want it to be actionable. Can we do this by mid-September? I will push hard to get a push report by Labor Day. Can we vote to go for trying to get the report out by Labor Day?

Brian: I agree.

Meeting adjourned. End of recording.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

HOMELAND SECURITY COMMISSION
QUARTERLY MEETING

441 4th Street, N.W.
Washington, DC 20001
Wednesday, February 26, 2020
2:00 pm to 4:00 pm
Room 1112 on Floor 11 South

Commission Member Attendees: Brad Belzak (Chair), Brian Baker, Joanna Turner, Phil McNamara, and Ed Pearson

HSEMA Attendee(s): Dion Black, Jason Rubinstein, and Abeer Sikder

Additional Attendees: Jamie Gorosh (Legislative Counsel, Committee on the Judiciary and Public Safety) and Steve Walker (Director, Mayor's Office of Talent and Appointments)

Note: No members of the public were present

Brad: Today is Feb 26, 2020. This is the first meeting since last May. I think I speak on behalf of all the commissioners in saying we're excited to be back, getting to work, working on ways to improve safety and security of the District, and move forward expeditiously in a collaborative nature. We're stronger together as a commission, working together with HSEM and across government. I'm excited to be here as your new chairman.

Before we begin, let's make some re-introduction.

Phil: Thank you Brad. Phil McNamara. I was previously with US Department of Homeland Security, currently on Pew Charitable trust. I'm excited to regroup.

Ed: I'm in the commission in my second year. I've been here years now, I retired from DC Fire. Let's get to work.

Joanna: I'm Joanna Turner. It's my second year of appointment of a 2-year commission appointment. I apologize for not being there in person.

Brian: Good afternoon. Appreciate letting me join by phone. I spend about 10 years with the District, in various roles in HSEMA. I'm excited to kick off the new agenda.

Brad: Before we move forward, I want to give a big thanks to David Heyman, who served as previous chair. I'm grateful for his service and the work he has done for the commission. I think I echo everyone's sentiments in getting the cyber report done. It was heavy lift, because we were

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

new to the commission. We benefited from David's leadership and we offer our heartfelt thank you. We wish him well and we'll stay in touch with him.

While we're still in the open session. I'm happy to have Jamie here. She's senior staffer to Councilmember Charles Allen. Helped craft legislation and passed it and ensures oversight for our commission. He's a great partner and plays a big role in securing the district and ensuring regulations are in place with a vision going forward.

Jamie, do you have anything to add?

Ms. Gorosh: Hi everyone. We've all met at some point. I'm Legislative Counsel for the Committee on the Judiciary and Public Safety. In the committee, I manage a cluster of 8 agencies and conduct oversight, HSEMA being one. I also have OCME, OUC, and some smaller core agencies. I'm excited to be here today, representing the council and committee. We want to take a more hands-on role in the process and be supportive. We take Homeland Security Commission reports seriously and we read them and acknowledge the important work you do. I'm excited to be here. Thank you for including me.

Phil: Mr. Chair, if I can. Jamie, thank you for coming over. I know you are perched over at Wilson building. Thank you for everything you and the chairman have done to get us all confirmed and reconfirmed.

I would like to ask a broad question, and if you feel comfortable sharing - looking into the mind of chairman Allen, with you as a proxy for him: what keeps you up at night? What are you most concerned about from a Homeland Security standpoint? What is Ward 6 saying to you?

Ms. Gorosh: It's not an exhaustive list. One concern is waterfront safety. Especially as people are moving there. We want waterways secure. I also heard this is something the commission takes up --- mass emergency events, like the Arthur Capper fire, impacting vulnerable populations and people with disabilities. Being prepared for those situations is vital. We need to prioritize having a plan in place for when something like this happens. This is a big priority in our office -- that is also what we want HSEMA prepared for. Those are two that initially stand out. I'll leave it there for now. Happy to continue engagement in the conversation and will talk to my boss if anything else is needed to be brought to the table.

Phil: To continue, I love the internet, because you can find almost everything. For example, through the DC Council legislative management system, I can get the entire package of my nomination.

I have a memo that Chairman Allen sent to the rest of council and it goes through what this nomination is all about, and about other commission members. I think it's important. There is a paragraph that jumped out—I want to have it read in open portion for the record. "Finally, the Committee would like to recognize and reinforce the Commission's independence from HSEMA. As an independent body, the Commission has the responsibility to make recommendations to

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Homeland Security Commission

Muriel Bowser
Mayor



Dr. Christopher Rodriguez
Director

improve the District's homeland security posture. This may result in recommendations that are critical of current District government practices. Constructive criticism is integral to the improvement and growth of HSEMA and all District agencies.”

As an independent body, we have power to make recommendations that may be critical of government agencies. That paragraph struck me. We are statutorily required to gather and evaluate information, measure progress and gaps and recommend improvement priorities. Sometimes when you make recommendations of what you can improve, you’re inherently saying that something needs to be improved. That may not always sit well with district officials.

We as an independent commission need to do an evaluation and use our collective expertise to say, in our judgment, this needs to be improved. We are not saying that to jam someone up. We are not saying that to cause waves. We’re saying that because we truly want to see the district prepared to respond to any type of incident. I really appreciate that paragraph in the chairman’s memo and want to note it in the record. Thank you again for coming down.

Brad: Thanks Phil, that was very helpful, and kind of really enforces why we’re here. Brian and Joanna – any comments?

Joanna: thank you Phil for comments. I totally agree.

Brian: Nothing to add.

Brad: Jamie, I just want to raise some points.

One, when we were confirmed the first time, Chairman Allen said resiliency was a big priority, along with waterfront security. We noted how important resiliency is, and how much I think, even before resilience came on the forefront -- now we are using the term in common place. But resiliency, is critical in a city like DC, where there is so much growth. Look back 15 years ago, there was really nothing on the waterfront. It was Georgetown Waterfront, Alexandria was building, but there was not a lot there - It wasn’t Anacostia, etc. etc. When I was confirmed 2 years ago this was something outright. That can mean many things – energy resiliency, security resiliency, etc.

I think what was striking was that Deputy Mayor made some points in our past meeting and we will touch upon this. I think this really resonates with what you are saying. This is something we should focus on and decide as a group.

Brian: Brad - I want to add to express importance of independence of commissions, and the importance of understanding that subject matter experts and professionals are here to be critical, and to further preparedness of homeland security and the district as a whole. I served with HSEMA. The district agencies in public safety are extremely competition. We’re fortunate to live in a place where public safety is important.